Department of Homeland Security

Office of Inspector General

Management Advisory Report: A Guide for Assessing Cybersecurity within the Office of Inspector General Community

Council of the Inspectors General on Integrity and Efficiency

This report was prepared on behalf of Council of the Inspectors General on Integrity and Efficiency.

OIG-14-43

February 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 24, 2014

MEMORANDUM FOR: Council of the Inspectors General on Integrity and Efficiency

FROM: Carlton I. Mann
Chief Operating Officer

SUBJECT: Management Advisory Report: *A Guide for Assessing Cybersecurity Within the Office of Inspector General Community*

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) tasked the Cybersecurity Working Group with undertaking a review in which it would examine the role of the Inspector General community in current Federal cybersecurity initiatives. CIGIE proposed that the Cybersecurity Working Group work under the auspices of the Information Technology (IT) Committee. As a member of the IT Committee, the Department of Homeland Security (DHS) Office of Inspector General (OIG) was asked to lead and coordinate the Cybersecurity Working Group's efforts in identifying the Inspector Generals' cybersecurity oversight role.

I am pleased to provide CIGIE with a high-level audit guide that can be used as a baseline for cyber and IT security-related reviews conducted by the Inspector General community. The guide is based on the subject matter expertise of DHS OIG IT audit managers and specialists, legal research, and a review of applicable websites and audit programs developed within the OIG community. The intent of this guide is to provide a foundation for conducting cybersecurity and IT system security-related audits. The guide was developed to the best knowledge available to DHS OIG. We trust that this guide will result in better protecting the integrity of Federal computer systems and networks and minimize the risks associated with cyber vulnerabilities and potential threats.

I would like to acknowledge the support provided to this effort by all the participants listed in Appendix X to produce a final document that represents the needs of the Inspector General community.

Attachment

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the *Inspector General Reform Act of 2008*, Public Law 110-409. The mission of the CIGIE is to—

- Address integrity, economy, and effectiveness issues that transcend individual government agencies.

- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Federal Inspector General (IG) community.

CIGIE Membership

- All IGs whose offices are established under either section 2 or section 8G of the *Inspector General Act*, or pursuant to other statutory authority (e.g., the Special IGs for Iraq Reconstruction, Afghanistan Reconstruction, and Troubled Asset Relief Program).

- The IGs of the Office of the Director of National Intelligence (or at the time of appointment, the IG of the Intelligence Community) and the Central Intelligence Agency.

- The IGs of the Government Printing Office, the Library of Congress, the Capitol Police, the Government Accountability Office, and the Architect of the Capitol.

- The Controller of the Office of Federal Financial Management.

- A senior-level official of the Federal Bureau of Investigation, designated by the Director of the Federal Bureau of Investigation.

- The Director of the Office of Government Ethics.

- The Special Counsel of the Office of Special Counsel.

- The Deputy Director of the Office of Personnel Management.

- The Deputy Director for Management of the Office of Management and Budget.

CIGIE Information Technology Committee

The CIGIE Information Technology (IT) Committee's mission is to facilitate effective IT audits, evaluations, and investigations by IGs, and to provide a vehicle for the expression of the IG community's perspective on Government-wide IT operations. Under its operating principles, this committee strives to promote participation by the IG community members in its activities, encourage communication and cooperation with colleagues in the IT field (including Federal Chief Information Officers and staff, and security professionals), and promote effective teamwork in addressing Government-wide initiatives, improving IG IT activities, and safeguarding national IT assets and infrastructure.

Some of the key activities of this committee include coordinating IT-related activities of the CIGIE, conducting relevant IT educational and training activities, advising the CIGIE on IT issues, and providing for IT information exchange among the IGs, including best practices and current capabilities. The Cybersecurity Working Group was formed under the auspices of the CIGIE IT Committee.

Table of Contents

Appendixes

Abbreviations

ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CD	compact disk
CERT/CC	Computer Emergency Response Team Coordination Center
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIKR	critical infrastructure and key resources
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CNCI	Comprehensive National Cybersecurity Initiative
COBIT	Control Objectives for Information and related Technology
CPR	Cyberspace Policy Review
CPU	Central Processing Unit
CVSS	Common Vulnerability Scoring System
DBMS	database management system
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	demilitarized zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
EAP	Extensible Authentication Protocol
EIMS	Enterprise Identity Management System

E-mail	electronic mail
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GAO	U.S. Government Accountability Office
GID	group identification
HP	Hewlett-Packard
HSPD	Homeland Security Presidential Directive
HSR	Homeland Security Roundtable
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAO	Information Assurance Officer
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ID	identification
IDPS	intrusion detection and prevention system
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IG	Inspector General
IP	Internet Protocol
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
IT	information technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NFS	Network File System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSA	U.S. National Security Agency
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget

OWASP	Open Web Application Security Project
PCI	PIV Card Issuer
PDD	Presidential Decision Directive
PII	personally identifiable information
PIV	Personal Identity Verification
RAM	random access memory
RAT	Router Auditing Tool
RFID	Radio Frequency Identification
RMF	Risk Management Framework
ROE	Rules of Engagement
ROM	read-only memory
SANS	SysAdmin, Audit, Network, Security
SDRAM	synchronous dynamic random access memory
smb	server message block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
UUCP	UNIX-to-UNIX-Copy
VLAN	virtual local area network
VPN	Virtual Private Network
VTL	Virtual Terminal Line
VTP	VLAN Trunking Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	wireless fidelity
WLAN	wireless local area network

Executive Summary

Securing cyberspace is an extraordinarily difficult challenge that requires a coordinated and focused effort from our entire society. The borderless nature of threats to, and emanating from, cyberspace requires robust engagement and strong partnerships with countries around the world. Cybersecurity risks pose some of the most serious economic and national security challenges our Nation faces. Cybersecurity involves the protective measures taken to secure cyberspace and its associated infrastructure, as well as the restoration of information systems and the data contained therein to ensure system confidentiality, integrity, and availability. It also aims to protect computers and networks from accidental or malicious harm by preventing, detecting, and responding to risks and attacks. Protection from the threat of cyber attacks is essential to the resilience and reliability of the Nation's critical infrastructure and key resources and, therefore, to our economic and national security.

In the fall of 2010, the Council of the Inspectors General on Integrity and Efficiency asked the Department of Homeland Security Office of Inspector General to lead a Cybersecurity Working Group. The Cybersecurity Working Group was charged with undertaking a two-part review, in which it would (1) identify recommended best practices for maintaining the integrity of Inspector General information technology systems and protecting them against threats and vulnerabilities and (2) examine the role of the Inspector General community in current Federal cybersecurity initiatives.

A report that addressed part one of the Council of the Inspectors General on Integrity and Efficiency's undertaking was published in September 2011. The second part of this effort focuses on the Inspector General's cybersecurity oversight role. Specifically, the Council of the Inspectors General on Integrity and Efficiency Cybersecurity Working Group, operating under the auspices of the Information Technology Committee, was tasked with developing a high-level audit guide that can be used as a baseline for cyber and information technology security-related reviews conducted by the Inspector General community. The Department of Homeland Security Office of Inspector General, a member of the Information Technology Committee, was asked to coordinate the Cybersecurity Working Group's efforts.

As part of this effort, we collected cybersecurity and information technology system audit plans and programs from several agency Offices of the Inspector General. These plans and programs, in part, are consolidated in this guide. The guide will assist information technology auditors in evaluating the cybersecurity policies, practices, and system security controls implemented to protect Federal computer systems and networks from cyber threats and vulnerabilities. It also cites established policies and guidance that can be used to evaluate critical information technology security controls. Further, the guide provides a foundation for conducting cybersecurity and information systems security-related audits that support Federal Information Security Management Act requirements.

The guide is divided into seven sections. The first section outlines Federal agency cybersecurity roles and responsibilities. The second section covers cybersecurity policies and guidance for evaluating critical information technology security controls. The next section focuses on guidance regarding the use of vulnerability assessments and penetration testing Inspector General audit organizations can perform to evaluate the effectiveness of the system security and access controls implemented, and determine how well systems are protected when subject to attacks. The fourth and fifth sections cover information security continuous monitoring and cloud computing respectively. The sixth section consists of program steps for evaluating an agency's cybersecurity program and initiatives. The last section outlines program steps for conducting information system security-related audits and evaluations.

Background

Cyberspace is composed of numerous interconnected computers, servers, routers, switches, and fiber optic cables that allow our Nation's critical infrastructures to work. Our Nation's economy and security are highly dependent on the global cyber infrastructure. We depend on a complex array of interdependent and critical networks, systems, and resources. The network of networks that supports the operation of all sectors of our economy can be disrupted both from inside and outside of the physical borders of the U.S. International engagement is a key element of U.S. efforts to safeguard and secure cyberspace.

The Internet is part of the cyber infrastructure and a strategic national asset. The Internet has been identified as a key resource, comprising domestic and international assets within both the information technology (IT) and communications sectors, and is used by all sectors to varying degrees. Protecting it is a national security priority. Attacks on our Nation's information networks can have serious consequences, such as disrupting critical operations, causing loss of revenue and intellectual property, or causing loss of life.

Recent foreign-based intrusions on the computer systems of U.S. Federal agencies and commercial companies highlight the vulnerabilities of the interconnected networks that comprise the Internet, and the need to address the global security and governance of cyberspace. The global aspects of cyberspace present key challenges to U.S. policy. Until these challenges are addressed, the U.S. will be at a disadvantage in promoting its national interests in the realm of cyberspace. Figure 1 documents the global cybersecurity challenges.

Figure 1: Challenges in Addressing Global Cybersecurity and Governance

Challenge	Description
Leadership	Providing top-level leadership that can coordinate across Federal entities and forge a coherent national approach.
Strategy	Developing a comprehensive national strategy that specifies overarching goals, subordinate objectives, and activities to support those objectives, and outcome-oriented performance metrics and timeframes.
Coordination	Engaging all key Federal entities in order to coordinate policy related to global aspects of cyberspace security and governance.
Standards and Policies	Ensuring that international technical standards and polices do not pose unnecessary barriers to U.S. trade.
Incident Response	Participating in international cyber incident response that includes appropriately sharing information without jeopardizing national security.
Differing Laws	Investigating and prosecuting transnational cybercrime amid a plurality of laws, varying technical capabilities, and differing priorities.
Norms	Providing models of behavior that shape the policies and activities of countries, such as defining countries' sovereign responsibility regarding the actions of its citizens.

Source: U.S. Government Accountability Office (GAO) analysis of Federal and non-Federal information (GAO-10-606).

Further, America's open and technologically complex society includes a wide array of critical infrastructure and key resources (CIKR) that are potential terrorist targets.[1] The Nation's critical infrastructure includes the distributed networks, varied organizational structures and operating models (including multinational ownership), independent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The majority of the Nation's CIKR are owned and operated by the private sector and State or local governments; CIKR are both physical and cyber-based and span all sectors of the economy. The national and economic security of the U. S. depends on the reliable functioning of the Nation's critical infrastructure. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.

Countering cyber threats and attacks requires the development of new risk mitigation capabilities if we are to:

- Reduce vulnerabilities.[2]
- Deter those with the capabilities and intent to harm our Nation's critical infrastructures.
- Ensure the confidentiality, integrity, and availability of our information and communications systems, and the sensitive data contained on these systems.

[1] Critical infrastructure is defined as those systems and assets—both physical and cyber—so vital to the U.S. that their incapacity or destruction would have a debilitating affect on national security, economic security, public health and safety, or any combination of those matters. Key resources are defined as publicly or privately controlled assets essential to the minimal operations of the economy and government.
[2] Vulnerabilities are defined as weaknesses in an information system, system security procedures, internal controls, or implementation, such as missing patches, service packs, open ports, and unnecessary services.

Objective and Scope

The purpose of this guide is to assist IT auditors in evaluating the cybersecurity policies, practices, and system security controls implemented to protect Federal computer systems and networks from cyber threats and vulnerabilities. The guide outlines the roles, responsibilities, and policies for cybersecurity oversight within the Federal Government. It also contains guidance on the use of vulnerability assessments and penetration testing OIG audit organizations can perform to evaluate the effectiveness of the system security and access controls implemented, and measure how well systems are protected when subject to attacks. Further, it provides a list of testing tools that can be used to evaluate critical IT security controls. Finally, the guide establishes program steps for evaluating cyber and IT security related audits. For example, the steps contained in this guide can be used to evaluate agencies' implementation of the Administration's top three priorities to improve cybersecurity:

1. Trusted Internet Connections.[3]
2. Continuous monitoring of Federal information systems and networks.[4]
3. Strong authentication controls/use of Personal Identity Verification (PIV) cards for logical access.

The steps in this guide are based on audits completed by members of the OIG community. They provide a baseline for conducting cyber and IT-related security evaluations, but they are not inclusive of all program steps that can be performed and controls that may be evaluated in conducting such audits. Additional steps and objectives can be added or modified as appropriate.

The scope of this document does not cover evaluation steps to address statutory Federal Information Security Management Act of 2002 (FISMA) requirements.[5] However, it contains audit steps for an assessment of agency-wide cybersecurity programs and information systems security that can be used to support FISMA requirements.

[3] The purpose of Trusted Internet Connections, as outlined Office of Management and Budget (OMB) Memorandum 08-05, is to optimize and standardize the security of individual external network connections currently in use by Federal agencies, including connections to the Internet. The initiative is to improve the Federal Government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections.
[4] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange systems, and environmental control systems.
[5] FISMA was enacted in 2002 as *Title III of the E-Government Act of 2002* to recognize the importance of information security to the economic and national security interests of the U.S.

Federal Agency Responsibilities

Responsibilities for cybersecurity are distributed across a wide array of Federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, issued in December 2003, directed DHS to serve as the Federal agencies' lead in assessing, mitigating, and responding to cyber risks in collaboration with Federal, State, and local governments, the private sector, academia, and international partners.[6] The Department was also responsible for leading efforts to protect and defend Federal civilian networks against cyber threats; coordinating response to cyber attacks and security vulnerabilities; and addressing the challenges to secure cyberspace, cyber assets, and our Nation's IT infrastructure.[7]

Presidential Decision Directive (PDD)-21, Critical Infrastructure Security and Resilience, issued in February 2013, advances a national unity of efforts to strengthen and maintain secure,[8] functioning, and resilient[9] critical infrastructure.[10] Through an updated and overarching framework that acknowledges the increased role of cybersecurity in securing physical assets, this directive focuses on actions to strengthen the security and resilience of critical infrastructure against evolving threats. Under this directive, which revokes HSPD-7, critical infrastructure security and resilience is to be a shared responsibility among Federal, State, local, tribal and territorial entities, and public and private owners and operators of critical infrastructure.

PDD-21 establishes national policy on critical infrastructure security and resilience, refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, and enhances overall coordination and collaboration. Additionally, the directive encourages the Federal Government to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the U.S. While greater information sharing within the

---

[6] http://www.dhs.gov/homeland-security-presidential-directive-7.
[7] The IT infrastructure consists of critical functions—sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (research and development, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.
[8] As defined in PDD-21, secure refers to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.
[9] Resilience refers to the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, including deliberate attacks, accidents, or naturally occurring threats or incidents.
[10] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

government and with the private sector is one of the three strategic goals of this directive, all Federal departments and agencies are to ensure that all privacy and civil liberties are respected.

DHS remains the focal point for coordinating best practices and supporting protective programs to secure cyberspace across and within government agencies under PDD-21. Further, DHS is responsible for providing the strategic guidance, promoting a national unity effort, and coordinating the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. As such, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance the protection of the critical infrastructure.

PDD-21 further defines the role of DHS in conjunction with the Department of Commerce, Department of Defense (DoD), Department of Justice (including the Federal Bureau of Investigation), Department of State, Federal Communications Commission, General Services Administration, Office of Science and Technology Policy, and other appropriate agencies with additional responsibilities for critical infrastructures. It also identifies 16 critical infrastructure sectors and designates the responsibility for those sectors to associated Federal Sector Specific Agencies. Figure 2 outlines the Federal agencies responsible for the protection of the various sectors and critical infrastructures.

Figure 2: Sector Specific Agencies and Critical Infrastructure Sectors

Sector Specific Agency	Critical Infrastructure Sectors
DHS	Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Emergency Services; IT; Nuclear Reactors, Materials, and Waste
DHS & General Services Administration	Government Facilities
DHS & Department of Transportation	Transportation Systems
Department of Health and Human Services	Healthcare and Public Health
U.S. Department of Agriculture & Department of Health and Human Services	Food and Agriculture
Environmental Protection Agency	Water and Wastewater Systems
Department of Energy	Energy
Department of the Treasury	Financial Services
DoD	Defense Industrial Base

Source: PDD-21.

All Federal departments and agencies are responsible for the identification, prioritization, assessment, remediation, and security of their respective critical infrastructure that supports primary mission essential functions. Consistent with FISMA, agencies are to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.[11]

[11] Information security pertains to protecting the confidentiality and integrity of data and ensuring data availability.

FISMA emphasizes the need for each agency to develop, document, and implement an agency-wide information security program to provide a high level of security for the information and information systems that support agency operations and assets. It provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA also requires that personnel, including contractors and other users of information systems, be trained so that they are aware of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks.

In July 2010, the Office of Management and Budget (OMB) issued Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*. In the memorandum, while OMB acknowledges that it still has a number of cybersecurity responsibilities principally in connection with FISMA, OMB clarifies that DHS is to exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity for the those information systems that fall within FISMA.

Cybersecurity Policy

As defined, cybersecurity comprises the collection of policies, security concepts and safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. The general security objectives comprise availability and integrity (that may include authentication, non-repudiation, and confidentiality). In addition, cybersecurity includes the full range of threat and vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies.

Different types of cyber threats may use various exploits to affect computers adversely, software, networks, agencies' operations, industries, or the Internet. Cited guidance outlining the responsibilities for securing cyberspace and CIKR follows.

The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace was issued in February 2003 to help reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures and the physical assets that support them.[12] The *Strategy* provides an initial framework for both organizing and prioritizing Federal agencies' roles in securing cyberspace. It focuses on improving the national response to cyber incidents, reducing threats and vulnerabilities to potential exploits, preventing cyber attacks against critical U.S. infrastructure, and improving the international management of and response to such risks and harm.

As outlined in *The National Strategy to Secure Cyberspace*, the need to secure cyberspace is a global matter due to the interconnectedness of the world's computer systems. The global interconnectivity provided by the Internet allows malicious users to easily cross national borders, affect large numbers of individuals, and maintain anonymity.

National Infrastructure Protection Plan

The National Infrastructure Protection Plan (NIPP), revised in 2009, provides the unifying structure to integrate existing and future CIKR.[13] It addresses the protection of the cyber elements of CIKR in an integrated manner rather than as a separate consideration. Our Nation's economy and national security are highly dependent on the global cyber infrastructure, which has created an interconnected and interdependent global network. The

[12] http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
[13] http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

global network links the physical and cyber elements of CIKR. Cyber interdependence presents a unique challenge for all sectors. The security and effective operation of U.S. critical infrastructure rely on cyberspace, industrial control systems, and IT that may be vulnerable to disruption or exploitation.

Comprehensive National Cybersecurity Initiative

Launched by the White House in January 2008 in National Security Presidential Directive 54/HSPD-23, the Comprehensive National Cybersecurity Initiative (CNCI) consists of 12 mutually reinforcing initiatives designed to help secure the U.S. in cyberspace.[14] Its goals include (1) managing the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections; (2) deploying an intrusion detection and prevention system (IDPS) of sensors across the Federal enterprise to enhance shared situational awareness of network vulnerabilities, threats, and events in the Federal Government and to act quickly to reduce our current vulnerabilities and prevent intrusions; (3) enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key IT; (4) strengthening the future cybersecurity environment by expanding cyber education, coordinating and redirecting research and development efforts across the Federal Government, and working to define and develop strategies to deter hostile or malicious activity in cyberspace; and (5) defining the Federal role for extending cybersecurity into critical infrastructure domains.

Cyberspace Policy Review

Recognizing the challenges and opportunities inherent in securing cyberspace, President Obama identified cybersecurity and the establishment of related performance metrics as key management priorities of his administration. Shortly after taking office, the President directed a 60-day comprehensive review to assess U.S. policies and structures for cybersecurity, known as the Cyberspace Policy Review (CPR).[15] The CPR recommends that the U.S. work actively with all countries to develop a trusted, safe, and secure cyber infrastructure that enables prosperity for all nations. Upon completion of the review, the Commission on Cybersecurity for the 44th Presidency issued a report, titled *Assuring a Trusted and Resilient Information and Communications Infrastructure*, in May 2009.

International Strategy for Cyberspace

To address the recommendations made in the CPR, the White House released the *International Strategy for Cyberspace* in May 2011.[16] The *Strategy* outlines the Nation's approach to unify

[14] http://www.whitehouse.gov/cybersecurity/comprehensivenational-cybersecurity-initiative.
[15] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[16] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

our engagement with international partners on a full range of cyber issues. It calls for the U.S. to work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens security, and fosters free expression and innovation to reduce the threats we face.

Because of cybersecurity's borderless nature, it is essential that foreign governments and international organizations play an active role in developing cyberspace security policies and procedures aimed at improving collaboration, information sharing, and incident response capabilities. As the Internet's core functionality relies on systems of trust, the international community needs to recognize the implications of its technical decisions and act with respect for one another's networks with the broader interest of preserving global network functionality and improving security.[17]

Department of Defense Strategy for Operating in Cyberspace

Along with the rest of the U.S. Government, DoD depends on cyberspace to function. DoD operates more than 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations. Furthermore, DoD operations—both at home and abroad—are dependent on the critical infrastructure.

Issued in July 2011, the *Department of Defense Strategy for Operating in Cyberspace* focuses on cyber threats that include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD's operational ability.[18] DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action, including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems. The strategy contains five initiatives: (1) take advantage of cyberspace's potential; (2) employ new defense operating concepts to protect DoD networks and systems; (3) partner with other government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy; (4) build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; and (5) leverage the Nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

[17] Systems of trust are systems that can be relied upon, to a specified extent, to enforce a specified security policy. Trusted systems are used for the processing, storage, and retrieval of sensitive or classified information.
[18] http://www.defense.gov/news/d20110714cyber.pdf.

Executive Order 13636

To strengthen the resilience of the critical infrastructure, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, on February 12, 2013.[19] This directive calls for the development of a "Cybersecurity Framework" that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to assist organizations responsible for critical infrastructure with services to manage cybersecurity risk. It also calls for partnerships with the owners and operators of critical infrastructure, to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, DHS, in collaboration with DoD, are to establish procedures to expand the Enhanced Cybersecurity Services program, a voluntary information sharing program, to all critical infrastructure sectors. The program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0

In response to Executive Order 13636, on February 12, 2014, the National Institute of Standards and Technology (NIST)[20] released the *Framework for Improving Critical Infrastructure Cybersecurity*.[21] The Framework, developed in collaboration with industry, provides guidance to an organization on reducing and better managing cybersecurity risks. It is focused on supporting the improvement of cybersecurity for the Nation's critical infrastructure using industry-known standards and best practices.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. It consists of three parts:

1. Framework Core - The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles.

---

[19] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[20] NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but do not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over those systems.
[21] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

2. Framework Profile - Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.
3. Framework Implementation Tiers - The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. It can also assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the U.S. and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

Appendix A of this guide contains additional references to relevant cybersecurity directives and guidance.

System Security and Vulnerability Guidance

It is imperative to implement adequate logical security controls on Federal agencies' information systems to ensure that the integrity and reliability of the information processed, stored, and transmitted is not compromised. Continually monitoring Federal agency networks for abnormalities is essential to minimize the risks of potential cyber attacks. Further, physical security controls are needed to protect the systems from unauthorized access, misuse, or destruction.

Adequate security controls mitigate the risks and vulnerabilities incurred by the use of information and information systems in the performance of Federal agency missions and business functions. Risks and vulnerabilities need to be analyzed and their potential effect measured. Vulnerabilities should be remediated, mitigated through compensating controls, or documented, with the organization accepting the potential risk.

Several different entities publish information security standards and baselines for various information systems, networks, platforms, software, and other products. Below are common sources used to audit Federal agency system and network security. The sources listed provide minimum security requirements, baselines, configuration settings, and checklists that can be used to evaluate the controls that should "lock down" information systems, networks, and software that might otherwise be vulnerable to attack. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

NIST Special Publication 800-53 - *Security and Privacy Controls for Federal Information Systems and Organizations* (Revision 4)

NIST Special Publication (SP) 800-53, Revision 4, was developed in April 2013 to further NIST's statutory responsibilities under FISMA.[22] It was written as part on an ongoing effort to produce a unified information security framework for the Federal Government. The purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the Federal Government and to meet all the requirements of Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information Systems* (see

[22] http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Appendix A).[23] The guidelines apply to all components of an information system that process, store, or transmit Federal information.[24]

This special publication provides a catalog of security controls and privacy standards for Federal information systems and organizations.[25] It also outlines a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats that include hostile cyber attacks, natural disasters, structural failures, and human errors.[26] Additionally, the publication contains guidance on multitiered risk management, security control baselines, and external service providers.

The security and privacy controls contained in NIST SP 800-53 are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. Both of the types of controls outlined in this publication are designed to facilitate compliance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

The catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Security controls are organized into 17 families based on the domain areas of the security requirements. The control families are grouped into three broad classes – technical, operational, and management. See Figure 3 for the control families and classes.

Figure 3: Security Control Families and Classes

Technical	Operational	Management
Access Control Audit and Accountability Identification and Authentication System and Communication Protection	Awareness and Training Configuration and Management Contingency Planning Incident Response Maintenance Media Protection Physical and Environmental Protection Personnel Security System and Information Integrity	Certification, Accreditation and Security Assessment Planning Risk Assessment System and Services Acquisition

Source: NIST SP 800-146.

[23] The term organization describes an entity of any size, complexity, or positioning within an organizational structure (e.g., Federal agency or, as appropriate, any of its operational elements).
[24] Information system components include for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, operating systems, virtual machines, middleware), and applications.
[25] The privacy controls are based on international standards and best practices that help organizations enforce privacy requirements derived from Federal legislation, directives, policies, regulations and standards.
[26] Organizational operations include mission, functions, image, and reputation.

The catalog of privacy controls is intended to:

- Establish a linkage and relationship between privacy and security controls for the purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within Federal information systems, programs, and organizations.
- Demonstrate the applicability of the NIST Risk Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in Federal information systems, programs and organizations.
- Promote closer cooperation between privacy and security officials within the Federal Government to help achieve the objectives of senior leaders/executives in enforcing the requirements in Federal privacy legislation, policies, regulations, directives, standards, and guidance.

NIST SP 800-61 - *Computer Security Incident Handling Guide* (Revision 2)

Computer security incident response has become an important component of IT programs. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. FISMA requires Federal agencies to establish incident response capabilities. In addition, each Federal civilian agency must contact the U.S. Computer Emergency Readiness Team (US-CERT) and report all incidents consistent with the agency's incident response policy.[27]

Performing incident response effectively is a complex undertaking; establishing a successful incident response capability requires substantial planning and resources. NIST SP 800-61, Revision 2, issued in August 2012, assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.[28] This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. According to NIST SP 800-61, effective incident response has four phases: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity (see figure 4).

[27] Under DHS, US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.
[28] http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

Figure 4: Incident Response Life Cycle

Source: NIST SP 800-61.

<u>NIST SP 800-94</u> - *Guide to Intrusion Detection and Prevention Systems*

IDPSs have become a necessary addition to the security infrastructure of nearly every organization. NIST SP 800-94, issued in February 2007, defines intrusion detection as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.[29] Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. An intrusion prevention system is software that has all the capabilities of an intrusion detection system (IDS) and can also attempt to stop possible incidents.

IDPSs are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use these systems for other purposes, such as identifying areas of noncompliance with security policies, documenting existing threats, and deterring individuals from violating security policies. Intrusion detection and prevention technologies offer many of the same capabilities, and administrators can usually disable prevention features in intrusion prevention products, causing them to function as IDSs.

The types of IDPS technologies are differentiated primarily by the types of events they monitor and the ways in which they are deployed. NIST SP 800-94 discusses four types of IDPS technologies:

- Network-Based – Monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
- Wireless – Monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves.
- Network Behavior Analysis – Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems).

[29] http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

- Host-Based – Monitors the characteristics of a single host (e.g., computer, laptop) and the events occurring within that host for suspicious activity.

Security Technical Implementation Guides

The Defense Information Systems Agency (DISA), a component of DoD, has defined baselines called Security Technical Implementation Guides (STIGs) [30] to lockdown information systems and software that might otherwise be vulnerable to attack.[31] STIGs are information security guides that contain a compendium of DoD policies, security regulations, and best practices for securing an information assurance or information assurance-enabled device (operating system, network, application software, etc.). The STIG website contains links to numerous security baselines for operating systems, applications, and telecommunication equipment. STIGs can assist agencies in producing security baselines for the products they use.

US-CERT

US-CERT was created as the focal point to protect the Nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. Its information sharing and incident response process includes distributing recipient-specific Department/Agency Cybersecurity Activity Reports to Federal agencies.[32] Additionally, as part of these responsibilities, each week, US-CERT provides Cyber Security Bulletins[33] that summarize new vulnerabilities that have been recorded by NIST in the National Vulnerability Database (NVD).[34] The bulletins are compiled from external, open source reports, not directly from results of US-CERT analyses.

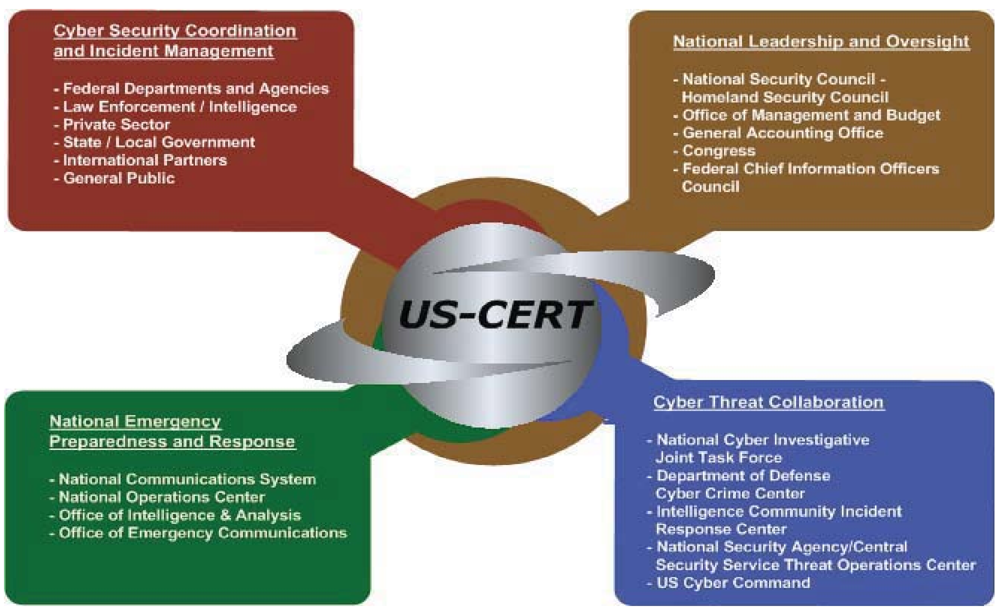
The NVD is the U.S. Government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol.[35] This data enables the automation of vulnerability management, security measurement, and compliance. The NVD also includes databases of security checklists, security-related software flaws, misconfigurations, product names, and metrics. Further, the NVD contains historical vulnerability information; the vulnerabilities are based on the Common Vulnerability and

[30] http://iase.disa.mil/stigs/.
[31] System lockdown is a protection setting that can be used to control applications that that are authorized to run on a client computer. It ensures that an organization's system stays in a known and trusted state and can be used to block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application.
[32] US-CERT publishes the weekly Department/Agency Cybersecurity Activity Reports to provide senior cybersecurity officials awareness of cybersecurity incidents occurring across the civilian Federal Government. These reports detail the trends observed in the .gov domain and open source reporting.
[33] http://www.us-cert.gov/alerts-and-tips/.
[34] http://nvd.nist.gov/.
[35] The Security Content Automation Protocol is a synthesis of interoperable specifications derived from community ideas.

Exposures naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard.[36] Vulnerabilities are listed as high, medium, or low based upon their severity and corresponding CVSS score. The NVD provides CVSS scores for almost all known vulnerabilities. Patch information is provided when available.[37]

US-CERT collaborates with Federal agencies, the private sector, the research community, State, local, and tribal governments, and international entities. Through coordination with various national security incident response centers responding to incidents on both classified and unclassified systems and related analysis, US-CERT disseminates reasoned and actionable cyber security information to the public. Figure 5 illustrates US-CERT's operating environment, which aims to initiate two-way exchanges in order to collect incident information that may affect the Nation's cyber infrastructure.

Figure 5: US-CERT's Operating Environment



Source: US-CERT.

Industrial Control Systems CERT

Control systems are vital to the operation of the U.S. critical infrastructures, which are often highly interconnected and mutually dependent systems. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence

[36] http://nvd.nist.gov/cvss.cfm.
[37] A patch is an additional piece of code developed to address problems (commonly called "bugs") in software.

community and coordinating efforts among Federal, State, local, and tribal governments, as well as control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector computer emergency response teams to share control systems-related security incidents and mitigation measures.

ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies. ICS-CERT is a key component of the *Strategy for Securing Control Systems*. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. ICS-CERT leads this effort by:

- Responding to and analyzing control systems-related incidents.
- Conducting vulnerability, malware, and digital media analysis.
- Providing on-site incident response services.
- Providing situational awareness in the form of actionable intelligence.
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations.
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

ICS-CERT provides on-site incident response, free of charge, to organizations that require immediate investigation and resolution in responding to a cyber attack. Further, ICS-CERT maintains and operates a malware lab, which provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. ICS-CERT collaborates with US-CERT, bringing technical expertise and incident response capabilities related to industrial control systems security to the partnership. Their work is performed with US-CERT and supports their overall mission to coordinate defense against and response to cyber attacks across the Nation. ICS-CERT publishes security bulletins in conjunction with US-CERT (http://ics-cert.us-cert.gov/alerts).

SysAdmin, Audit, Network, Security Institute

The SysAdmin, Audit, Network, Security (SANS) Institute[38] has identified 20 critical IT security controls that organizations should implement for effective cyber defense.[39] These controls, the *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines*, were

[38] http://www.sans.org/.
[39] The SANS Institute is a well-known cooperative research company that develops and maintains the largest collection of research documents about various aspects of information security and operates the Internet Storm Center, the Internet's early warning system. Reference to the SANS Institute, a private organization, is made for informational purposes only and does not constitute an endorsement by CIGIE or any Federal agency. Moreover, it does not imply that its recommendations are necessarily the most appropriate or best available.

agreed upon by a powerful consortium that includes the National Security Agency (NSA), US-CERT, DoD, the Departments of Energy and State, and the top commercial forensics experts and penetration testers that serve the banking and critical infrastructure communities.

The consortium produced a document that identifies the 20 specific technical security controls effective in blocking currently known high-priority attacks, as well as attack types expected in the near future. The top 20 controls are not intended to be comprehensive and do not replace the numerous controls outlined in NIST SP 800-53. Rather, they represent a starting baseline, part of the recognition that complete security is neither possible nor necessary. Each of the 20 control areas includes multiple individual subcontrols that specify actions an organization can take to help improve its defenses. The control areas and individual subcontrols focus on various technical aspects of information security, with the primary goal of helping organizations prioritize their efforts to defend against today's most common and damaging computer and network attacks. The SANS Institute recommends that Federal agencies examine all 20 control areas against the current agency status and develop an agency-specific plan to implement the controls as a key component of an overall IT security program. Figure 6 lists the control areas.

Figure 6: Twenty Critical Security Controls for Effective Cyber Defense

Security Controls	
Inventory of Authorized and Unauthorized Devices	Controlled Use of Administrative Privileges
Inventory of Authorized and Unauthorized Software; Enforcement of "White" Lists of Authorized Software	Limitation and Control of Ports, Protocols, and Services
Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Maintenance, Monitoring, and Analysis of Complete Audit Logs
Continuous Vulnerability Testing and Remediation	Boundary Defense
Anti-Malware Defenses	Controlled Access Based on Need to Know
Application Software Security	Dormant Account Monitoring and Control
Wireless Device Control	Data Leakage Prevention
Data Recovery Capability (validated manually)	Red Team Exercises
Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)	Secure Network Engineering (validated manually)
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Incident Response Capability (validated manually)

Source: SANS Institute.

Sources for Additional Guidance

According to the Center for Internet Security (CIS), sources for additional best practice standards, frameworks, and guidelines for IT security include:[40]

- Control Objectives for Information and related Technology (COBIT)
  COBIT includes generally accepted best practices, processes, measures, and indicators for IT governance and control (http://www.isaca.org).

- International Standardization Organization/International Electrotechnical Commission 27001 IT Security techniques - Information security management systems
  Together, these techniques provide a comprehensive management system for information security focused on IT risk and controls (http://www.iso.org).

- CIS Benchmarks
  CIS provides best practice standards and benchmarks to control IT risks, with a focus on technical security benchmarks, configurations, and metrics (http://cisecurity.org).

- Open Web Application Security Project (OWASP)
  OWASP provides web and application security best practices and tools (http://www.owasp.org).

- NSA Guides
  These technical security configuration guides developed and used by NSA cover a wide range of technologies (http://www.nsa.gov/ia/guidance/security_configuration_guides/).

- Information Technology Infrastructure Library (ITIL)
  The ITIL is a comprehensive set of best practices for IT services management (problem, change, configuration, and incident management), development, and operations (http://www.itil-officialsite.com).

Appendix A contains additional references to relevant system security and vulnerability guidance.

[40] CIS is a nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, with a commitment to excellence through collaboration. Through its four divisions—Security Benchmarks, Multi-State Information Sharing & Analysis Center, Trusted Purchasing Alliance, and the Integrated Intelligence Center—CIS serves as a central resource in the development and delivery of high-quality, timely products and services to assist government, academia, the private sector, and the general public in improving their cyber security posture.

System Vulnerability Management and Penetration Testing

In today's Federal IT environment, it is essential that organizations maintain a strong and secure information security program. One of the biggest security challenges Federal agencies encounter today is protecting their information systems against malicious attacks from both internal and external threats. The exploitation of vulnerabilities via the Internet is a huge problem requiring immediate proactive control and management. Vulnerabilities that have plagued operating systems and software applications from the earliest days of computing are identified on a daily basis. Further, reliance on a global IT supply chain introduces multiple risks to Federal information systems. These risks may include threats posed by foreign intelligence services or counterfeiters, who may exploit vulnerabilities, thereby compromising the confidentiality, integrity, or availability of an end system and the data it contains. These risks can also have an adverse effect on an agency's ability to carry out its mission. Appendix B contains a list of the top system threats for 2013 and beyond.

Vulnerability management is the practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems. As the Federal Government works to protect its information systems and networks, it is important that system vulnerabilities be identified and prioritized for remediation. Once vulnerabilities are identified, it is equally important to test systems to determine whether these vulnerabilities can be exploited to gain unauthorized access to the system or network. Vulnerabilities need to be analyzed and their potential impact measured. Vulnerabilities should be remediated, mitigated through compensating controls, or documented, with the potential risk to the organization accepted. OIG audit organizations can perform vulnerability assessments and penetration testing to evaluate the effectiveness of the system security and access controls implemented, and measure how well systems are protected when subject to attacks.

Vulnerability Assessment

When exposed, vulnerabilities can be targeted for exploitation by a threat source. A vulnerability assessment is a formal description and evaluation of the vulnerabilities in an information system. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system.
2. Assigning quantifiable value (or at least rank order) and importance to those resources.
3. Identifying the vulnerabilities or potential threats to each resource.
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources.

Scanning is the foundational process in conducting a vulnerability assessment. System scans test the effectiveness of the security policy and controls by examining the network infrastructure for vulnerabilities by systematically testing and analyzing Internet Protocol (IP) devices, services, and applications for known security weaknesses. Scans can also test for compliance with system and network configuration requirements.

Proper planning is critical to any successful security assessment. Prior to launching a scan, the audit team should have a Rules of Engagement (ROE) in place with agency management to define what will be tested, how the testing will be conducted, the names of the agency monitor(s) who will observe the testing, the system location(s) for testing, and a list of scanning/testing tools. Prior to beginning testing, the ROE should be agreed to and signed off on by agency and OIG management. The ROE should also document the individuals to contact in the event of disagreement(s) during testing and the process to be followed should a significant event occur during testing that would result in the OIG test team or the agency requesting that the testing be terminated. The agency's monitor(s) should have the knowledge and understanding of the significant events that would lead the agency to direct the OIG to terminate testing. A sample ROE is outlined in Appendix C.

At a minimum, the OIG team will need the IP (or IP ranges) for the agency's domains and sub-networks and the special access permissions needed to perform the testing. If the audit includes scanning specific devices, these devices should be identified by IP before the scan is launched. A list of what to scan may include the following:

- System/server/network operating systems.
- Web servers.
- Simple Mail Transfer Protocol (SMTP)/Post Office Protocol servers (i.e., electronic mail [E-mail] servers).
- File Transfer Protocol servers.
- Lightweight Directory Access Protocol (LDAP) servers.
- Domain Name System (DNS) servers.
- Load balancing servers.
- Workstations and laptops.
- Firewalls.
- Databases.
- Web applications.
- Network infrastructure appliances.
- Routers, switches, and hubs.
- Wireless access points (for signal leakage).

There are many options for scanning tools. Appendix D contains a list of automated scanning tools used by the IG community. The use of tools should be coordinated with the audit team and site personnel to determine the most appropriate tool for the platform being assessed.

Vulnerability assessment and management involve more than running scanning software on an application, computer, or network to detect common weaknesses. A security vulnerability assessment may also include:

- Determining whether agency requirements for system account access and security controls, including authentication procedures, have been implemented.
- Identifying the faults in software that affect security.
- Evaluating the effectiveness of the security controls implemented on operating systems, databases, and web applications.
- Determining whether separation of duties exists to restrict access to systems containing sensitive data.
- Ensuring that antivirus software and signatures are updated.
- Evaluating the software configurations for all security devices to evaluate compliance with the standard or required configuration.
- Ensuring that current security updates are applied on network-attached devices.
- Determining whether audit trails are being captured and monitored according to agency policy.
- Evaluating the agency's continuous monitoring strategy and process.
- Identifying the adequacy of the physical controls over the facilities where IT systems are housed.
- Documenting the state of security based on compliance with laws, regulations, and agency policy.

Subsequent to vulnerability testing, the vulnerabilities identified need to be analyzed and their potential significance measured. Each site or program should be given a list of the vulnerabilities and weaknesses identified during scanning, and the audit team should discuss any false positives that were identified by management.[41] The audit team and management should then discuss mitigation strategies for the remaining vulnerabilities. Vulnerabilities should be remediated, mitigated with compensating controls, or documented, with the potential risk to the organization accepted.

Penetration Testing

A more reliable way to identify the risk of vulnerabilities in aggregate is through penetration testing. Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data, using tools and techniques

[41] A false positive is any normal or expected behavior that is identified as anomalous or malicious. For example, a false positive can occur when a security scanner, such as Nessus, detects a specific vulnerability in an organization's program, but it is not a vulnerability. Sometimes the scanner signatures (the 'check logic') make mistakes and report a vulnerability that may not exist.

commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability. A penetration test captures in-depth vulnerability information at a single point in time.

Penetration testing can also be useful for determining:

- How well the system tolerates real-world-style attack patterns.
- The likely level of sophistication an attacker needs to compromise the system.
- Additional countermeasures that could mitigate or minimize threats against the system.
- Defenders' ability to detect attacks and respond appropriately.

Testing can be conducted in a number of ways and should first be discussed with management and defined in the ROE. For example, external security testing is conducted from outside the agency's security perimeter. This kind of testing offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the Internet—with the goal of revealing vulnerabilities that an external attacker could exploit. With internal security testing, an audit team can work from the internal network and assume the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited, and demonstrates the potential damage this type of attacker could cause. Internal security testing also focuses on system-level security and configuration, including application and service configuration, authentication, access control, and system hardening.

In addition to the way testing will be conducted, specific tests, constraints, tools, and systems to be tested should be discussed with agency management and documented in the ROE. Further, any potential legal concerns with an assessment should be taken into account and addressed before testing begins. While the involvement of legal advisors is at the discretion of the agency, it is recommended that they always be involved for intrusive tests such as penetration testing. Penetration testing involves a methodology that may attempt to (1) circumvent or defeat the security features of an application, system, or network, or (2) exploit identified or known system security vulnerabilities.

The four-stage penetration methodology is outlined below:

1. **Planning:** This phase covers information gathering and scanning. The assessment plan, or ROE, is developed in this phase.
2. **Discovery:** This is the vulnerability analysis phase and involves comparing the services, applications, and operating systems of scanned hosts against vulnerability databases (a process that is automatic for vulnerability scanners) and the testers' own knowledge of vulnerabilities. Written logs are usually kept and periodic reports are made to system administrators and/or management during this phase.

3. **Attack:** This phase is at the heart of any penetration test. It involves verifying previously identified potential vulnerabilities by attempting to exploit them. If an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure. As with discovery, written logs are usually kept during this phase to apprise system personnel and management of the testing status and results.
4. **Reporting:** At the conclusion of the test, a report is generally developed to describe identified vulnerabilities, present a risk rating, and provide and discuss guidance on how to mitigate the discovered weaknesses.

Penetration testing can be invaluable, but it is labor-intensive and requires great expertise to minimize the risk to targeted systems. Systems may be damaged or otherwise rendered inoperable during penetration testing, even though the agency benefits in knowing how a system could be rendered inoperable by an intruder. Although experienced penetration testers can mitigate this risk, it can never be fully eliminated. Penetration testing should be performed only after careful consideration, notification, and planning.

Penetration testing is usually conducted under specific constraints. It is important to be aware that depending on an agency's policies, the test team may be prohibited from using particular tools or techniques or may be limited to using them only during certain times of the day or days of the week. Results are valid only until the environment changes or new threats arise. Penetration testing often includes non-technical methods of attack and typically includes the following steps:

- **Network resource identification (ID)**: Sometimes called network mapping, network footprinting, or target ID. It involves scanning systems for open ports, identifying operating systems, and determining the types of applications that are operating on open ports.

- **Scanning for vulnerabilities**: Looking for vulnerabilities on server, firewall, and Voice Over IP operating systems. Tests designed to break the existing authentication scheme or database and web application controls can also be conducted. Once the audit team has finished with these tests, the resources identified are prioritized. Determining the significance of vulnerabilities is a complex task that requires considerable analytical thought. For example, any number of systems may have fairly serious vulnerabilities, but the audit team needs to assign certain systems a lower priority than others that are considered more vital, especially if a vulnerable system is not likely to become a stage for an attack.

- **Perimeter testing**: Firewall testing (see appendix R for evaluation steps).

- **Intrusion detection testing**: In this step, the audit team might generate traffic to determine whether the IDS is capable of identifying anomalies.

Audit trails are used to detect and deter penetration of a computer system and to reveal usage that identifies misuse. At the discretion of the system administrator, audit trails may be limited to specific events or may encompass all of the activities on a system.

- **Consideration of security policy and end user issues**: Determining the effectiveness of the security policy, and how well the network's applications ensure compliance. The team may also determine how well end users comply with the security policy. Although this step is not as relevant to applications, it is important to understand that an auditor does more than scan systems and generate packets.

Any vulnerabilities discovered during penetration testing should be remediated or mitigated with compensating controls if possible. A well-designed program of regularly scheduled network and vulnerability scanning, interspersed with periodic penetration testing, can help prevent many types of attacks and reduce the potential damaging effects of successful ones.

Information Security Continuous Monitoring

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, issued in September 2011, defines ISCM as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[42] NIST SP 800-137 specifically addresses the assessment and analysis of security control effectiveness and of organizational security status according to organizational risk tolerance. The purpose of this guideline is to assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides an awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls.

Any effort or process intended to support ongoing monitoring of information security across an organization begins with leadership defining a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people. The objective of an ISCM strategy is to conduct ongoing monitoring of the security of an organization's networks, information, and systems and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change. This strategy should:

- Provide a clear understanding of organizational risk tolerance and help officials set priorities and manage risk consistently throughout the organization.
- Include metrics that provide meaningful indications of security status at all organizational tiers.
- Ensure continued effectiveness of all security controls.
- Verify compliance with information security requirements derived from organizational missions/business functions, Federal legislation, directives, regulations, policies, and standards/guidelines.
- Include all organizational IT assets and help to maintain visibility into the security of the assets.
- Ensure knowledge and control of changes to organizational systems and environments of operation.
- Maintain an awareness of threats and vulnerabilities.

An ISCM program is established to collect information according to pre-established metrics, utilizing information readily available in part through implemented security controls. According to NIST, organizations should take the following steps to establish, implement, and maintain ISCM:

- Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business aspects.

[42] http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

- Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
- Analyze the data collected and report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
- Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- Review and update the monitoring program, adjusting the ISCM strategy, and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

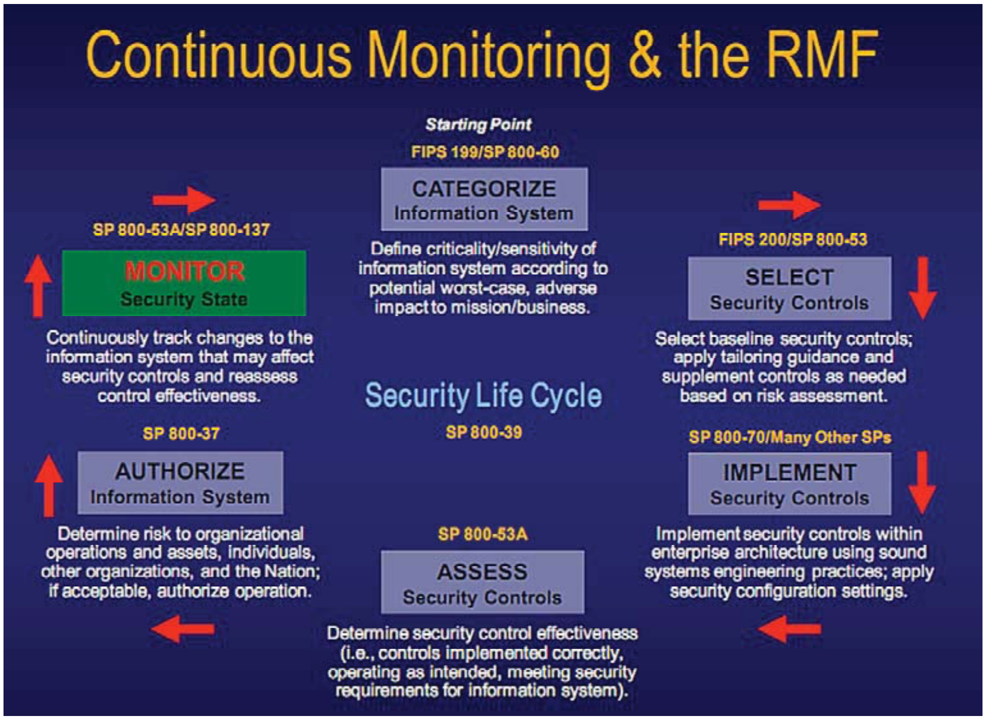
Overall, an effective continuous monitoring program is one that can adapt to the ever changing technology and cybersecurity threat landscape and encompasses vulnerability, application, and threat monitoring.

The importance of continuous monitoring is highlighted by NIST as one of the steps in its Risk Management Framework (RMF). The RMF developed by NIST describes a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle. Ongoing monitoring is a critical part of the risk management process and assessing an organization's information security posture. In the RMF, NIST defines the six components that work together to provide comprehensive guidance on how to implement continuous monitoring into the security lifecycle. Figure 7 outlines the components of the RMF, including continuous monitoring, in assessing an organization's overall state of security.

Continuous monitoring and real-time analysis of threats, while not new, are evolving concepts and are being implemented and deployed at various levels. While each organization's requirements are different, continuous monitoring should include the following types of both legacy and leading-edge monitoring and correlation capabilities:

- Vulnerability, configuration, and asset management.
- System and network log collection, correlation, and reporting.
- Advanced network monitoring using real-time network forensics.
- Threat intelligence and business analytics that fuse data from all monitoring feeds for correlation and analysis.

Figure 7: Assessing an Organization's Information Security Posture



Source: A Real-Time Approach to Continuous Monitoring (A SANS Whitepaper - February 2011).

The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance and the ability to provide the information needed to respond to risk in a timely manner. The result should be a picture of an IT system's status that can be used to maintain and improve an organization's information security posture and ensure compliance with NIST, FISMA, and other relevant guidance and requirements.

Real-time monitoring of implemented technical controls using automated tools and techniques can provide an organization with a much more dynamic view of the effectiveness of those controls and the security posture of the organization. According to NIST, a robust ISCM program enables organizations to move from compliance-driven risk management to data-driven risk management, providing organizations with the information necessary to support risk response decisions, status information, and ongoing insight into security control effectiveness.

FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency appropriate to risk, but no less than annually. The OIG community is also responsible for reviewing an agency's continuous monitoring process at least annually during their agency FISMA evaluations. Further, OMB's annual FISMA reporting instructions emphasize monitoring the security state of information systems on an ongoing basis with a frequency sufficient to make ongoing, risk-based decisions.

Cloud Computing

The present availability of high-capacity networks, low-cost computers and storage devices, in addition to the widespread adoption of hardware virtualization, service-oriented architectures, and utility computing have led to the growth in cloud computing.[43] Cloud computing allows computer users to conveniently rent access to fully featured applications, software development and deployment environments, and computing assets such as network-accessible data storage and processing. It is based on virtualization technology and focuses on the sharing of resources. The goal of cloud computing is to allow users to benefit from all technologies, without the need for in-depth knowledge or expertise with each one of them, thereby cutting costs, maximizing the effectiveness of shared resources, and helping users focus on their core business instead of being impeded by IT obstacles.

In February 2011, the White House issued the *Federal Cloud Computing Strategy*.[44] According to the strategy, cloud computing has the potential to significantly help agencies address its inefficiencies (e.g., low asset utilization, a fragmented demand for resources, and duplicative systems) and the need to provide highly reliable, innovative services quickly despite resource constraints. For the Federal Government, cloud computing holds tremendous potential to deliver public value by increasing operational efficiency and responding faster to user needs.

To harness the benefits of cloud computing, the White House instituted a Cloud First policy. This policy was intended to accelerate the pace at which the government would realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

Following the publication of the *Federal Cloud Computing Strategy*, each agency was to re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process. Consistent with the Cloud First policy, agencies were to modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. Agencies were to simplify their IT environments through the use of tools such as cloud computing and enterprise architectures to make them more manageable and then invest in the needed security to make them resilient.

The *Federal Cloud Computing Strategy* is designed to:

- Articulate the benefits, considerations, and trade-offs of cloud computing.
- Provide a decision framework and case examples to support agencies in migrating towards cloud computing.

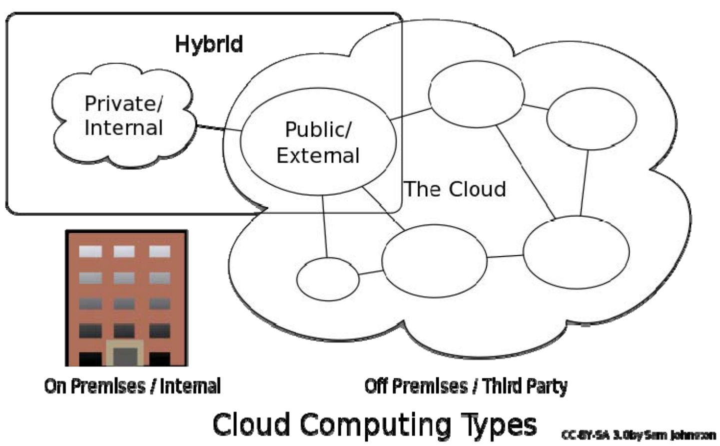
[43] Virtualization is the simulation of the software and/or hardware upon which other software runs.
[44] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

- Highlight cloud computing implementation resources.
- Identify Federal Government activities and roles and responsibilities for catalyzing cloud adoption.

NIST issued SP 800-145, *The NIST Definition of Cloud Computing*, in September 2011 to characterize the important aspects of cloud computing, serve as a means for broad comparisons of cloud services and deployment strategies, and provide a baseline for discussion of what cloud computing is and how best to use cloud computing.[45] In this publication, NIST defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model is composed of five essential characteristics: (1) on-demand self-service, (2) broad network access, (3) resource pooling, (4) rapid scalability and elasticity, and (5) measured service. The cloud may be owned, managed, and operated by an organization, a third party, or a combination of the two, and may exist on or off an organization's premises. Cloud computing providers offer their services according to three service models: infrastructure as a service, platform as a service, and software as a service. Further, cloud computing can be implemented using a variety of deployment models – private, community, public, or a hybrid combination. Figure 8 depicts the types of cloud computing.

Figure 8: Cloud Computing Types



Source: Wikipedia.

Cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments, and by applying innovations developed in the private sector. If an agency wants to launch a new innovative program, it can

[45] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

quickly do so by leveraging the cloud infrastructure without having to acquire significant hardware, lowering both time and cost barriers to deployment.[46]

By leveraging shared infrastructure and economies of scale, cloud computing presents a compelling business model for Federal leadership. Organizations will be able to measure and pay for only the IT resources they consume, increase or decrease their usage to match requirements and budget constraints, and leverage the shared underlying capacity of IT resources via a network. Resources needed to support mission critical capabilities can be provisioned more rapidly and with minimal overhead and routine provider interaction.

As cloud computing uses increase, it is likely that criminals will find new ways to exploit system vulnerabilities. While the cloud offers many strong points (e.g., infrastructure flexibility, faster deployment of applications and data, and cost control), several deterrents to widespread adoption of cloud computing remain. Among them, are reliability, availability of services and data, security, complexity, costs, regulations and legal issues, performance, migration, the lack of standards, limited customization, and data privacy issues.

When an organization subscribes to a cloud, all the data processed will physically reside in premises owned and operated by a service provider. Security concerns must be addressed to maintain trust in cloud computing technology. To mitigate the threat, cloud computing stakeholders will need to invest heavily in risk assessment to ensure that providers encrypt data, have established a foundation to secure the platform and infrastructure, and build higher assurance into auditing to strengthen compliance. NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, issued in December 2011, outlines security and privacy issues in depth for public clouds (see Appendix A).

To comply with regulations, including FISMA, OMB, in December 2011, directed Federal agencies to use a process called the Federal Risk and Authorization Management Program (FedRAMP) to assess and authorize cloud products and services.[47] FedRAMP consists of a subset of NIST SP 800-53 security controls specifically selected to provide protection in cloud environments.

The privacy and security of cloud computing depend primarily on whether the cloud service provider has implemented robust security controls and a sound privacy policy. In May 2012, NIST issued SP 800-146, *Cloud Computing Synopsis and Recommendations,* which explains cloud computing technology in plain terms and provides recommendations for IT decision makers.[48] According to NIST, cloud computing is a developing area and its ultimate strengths and

[46] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing.
[47] https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf
[48] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

weaknesses are not yet fully researched, documented, and tested. This publication provides recommendations on how and when cloud computing is an appropriate tool, and indicates the limits of current knowledge and areas for future analysis. Generally, NIST recommends that the following be considered in the context of cloud computing:

- **Management:** Mitigating data to and from clouds, continuity of operations, compliance, administrator staff, legal issues, operating policies, acceptable use policies, licensing, patch management
- **Data Governance:** Data access standards, data separation, data integrity, data regulations, data disposition, data recovery
- **Security and Reliability:** Consumer-side vulnerabilities, encryption, physical security, authentication, identity and access management, performance requirements, visibility
- **Virtual Machines:** Vulnerabilities, migration[49]
- **Software and Applications:** Time critical software, safety-critical software, application development tools, application runtime support, application configuration, standard programming languages

In July 2012, GAO reported that until agencies' cloud implementations are sufficiently planned and relevant systems are retired, the benefits of Federal efforts to implement cloud solutions—improved operational efficiencies and reduced costs—may be delayed or not fully realized.[50] Additionally, GAO identified seven common challenges associated with the implementation of the "Cloud First" policy:

1. Meeting Federal security requirements.
2. Obtaining guidance.
3. Acquiring knowledge and expertise.
4. Certifying and accrediting vendors.
5. Ensuring data portability and interoperability.
6. Overcoming cultural barriers.
7. Procuring services on a consumption (on-demand) basis.

[49] A virtual machine is an efficient, isolated duplicate of a real machine.
[50] INFORMATION TECHNOLOGY REFORM: *Progress Made but Future Cloud Computing Efforts Should be Better Planned* (GAO-12-756).

Steps for Evaluating a Cybersecurity Program

Over the past few years, threats in cyberspace have risen dramatically. Securing cyberspace involves reducing our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures. Ensuring that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage is an extraordinarily difficult challenge. The speed and anonymity of cyber attacks makes it difficult to distinguish among the actions of terrorists, criminals, and nation states; this task often occurs only after the fact, if at all.

Cybersecurity strives to ensure that an organization's systems and networks are protected against relevant security risks in the cyber environment. An organization's systems and networks include connected computing devices, infrastructure, applications, services, telecommunications capabilities, and information transmitted and stored. Addressing network security issues requires public-private partnerships as well as international cooperation and governing standards. A cybersecurity program encompasses the security controls used to protect the availability, integrity, and confidentiality of an organization's systems and networks, and the information stored on these computers. Federal agencies need to develop a plan to address the cybersecurity-related issues confronting the U.S.

The following areas should be considered when evaluating the effectiveness of an agency's cybersecurity program:

- Strategic cybersecurity and IT planning.
- Performance metrics.
- Information sharing and collaboration.
- Partnerships with counterparts in public, private, and international domains.

See appendix E for a list of audit objectives and steps that can be conducted in evaluating an agency's cybersecurity program.

Strategic Planning

PDD-21 instructs all Federal departments and agencies to identify, prioritize, and coordinate the protection of their own critical infrastructures in order to prevent, deter, or mitigate the effects of attacks. In addition, this national policy recognizes that certain other Federal entities have special functions related to critical infrastructure protection: DHS' responsibility for developing a comprehensive plan outlining the risk management framework, goals, and initiatives for strengthening the security and resiliency of critical infrastructure; Department of Justice's responsibilities for law enforcement activities across the critical infrastructure sectors; Department of State's responsibilities to engage with foreign governments and international organizations, and the Executive Office of the President's Office of Science and Technology's responsibilities to prioritize and guide research and development requirements and investments.

Further, *The National Strategy to Secure Cyberspace* provides a framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It also provides direction to Federal departments and agencies that have roles in cyberspace security and identifies steps that State and local governments, private companies, organizations, and individuals can take to improve our collective cybersecurity.

In addition, the *Government Performance and Results Act Modernization Act of 2010* requires the development of a strategic implementation plan that identifies an agency's major functions and operations. The plan should include general goals and objectives, describe how those goals and objectives can be achieved, and cover at least 4 years following the fiscal year in which the plan is developed.

Without a strategic implementation plan for cybersecurity, given the complexity of protecting cyberspace, it is difficult for an agency to achieve its IT goals and objectives. It is crucial that a comprehensive implementation plan be developed to provide the necessary guidance to work with appropriate stakeholders to meet the requirements specified in *The National Strategy to Secure Cyberspace*.

Performance Metrics

Closely tied to strategic planning are performance metrics. The use of performance metrics is a critical step in the risk management process to enable DHS and Sector-Specific Agencies to assess improvements in CIKR protection and resiliency at the national and sector levels objectively and qualitatively. Performance metrics allow an organization to track progress against priorities, establish accountability, document actual performance, promote effective management, and provide for a method to advise decision makers. Performance metrics indicate what a program is accomplishing and whether results are being achieved. In addition, measures help management determine how to allocate resources and evaluate the effectiveness of current efforts.

The *Government Performance and Results Act Modernization Act of 2010* requires Federal agencies to establish performance goals as well as metrics that assess relevant outputs, service levels, and outcomes of each program activity. OMB requires each agency to prepare an annual performance plan covering each program activity included in its budget. A performance plan should include the following:

- Goals that define the level of performance to be achieved by a program activity.
- Goals that are objective, quantifiable, and measurable.

- Performance indicators to measure or assess the relevant output, service levels, and outcomes of each program activity.
- A basis for comparing actual program results with established performance goals.

Measuring performance allows organizations to track their progress toward their goals and gives managers crucial information on which to base their organizational and management decisions. For example, performance metrics are valuable to management when forecasting future budgetary needs. Leading organizations also recognize that performance measures can create powerful incentives to influence organizational and individual behavior. Additionally, when appropriate, making performance measurements available to the public demonstrates transparency, allowing the public to see evidence of program effectiveness.

Information Sharing and Collaboration

PDD-21 requires DHS and other Federal agencies, as well as State and local governments, to collaborate with the private sector to facilitate information sharing concerning physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices in a timely manner. Additionally, the CNCI encourages increased information sharing between the Federal Government and the public and private sector owners and operators of the CIKR.

The NIPP of 2009 encourages effective communication, which includes multidirectional information sharing between government and industry, to streamline and reduce redundant reporting. The plan establishes a goal that requires CIKR partners to strive toward access to robust information sharing networks that include relevant intelligence and threat analysis, and incident reporting.

Interaction among all levels of government, the private sector, and our international partners can enhance the measures taken and decisions made to improve and protect cyberspace. It is difficult to exchange cyber data among government organizations, and with industry, academia, international partners, and government counterparts, without an information sharing policy. Additionally, without continued engagement and commitment to address cyberspace and IT system security issues, there is increased risk that cyber threat information sharing will be severely limited. Further, inadequate communication and information sharing can restrict the ability to develop the trust-based relationships required to share and receive actionable cyber threat information.

Public/Private/International Partnerships

The protection of our critical infrastructures is necessarily a shared responsibility and requires partnerships between owners, operators, and the government. Approximately 90 percent of critical infrastructure is privately owned and operated. Public-private partnerships are essential for developing trusted, two-way information sharing that is crucial to improve and protect cyberspace.[51] Furthermore, the Federal Government needs to encourage international cooperation to help manage this increasingly global problem.

The CNCI encourages the enhancement of partnerships between the Federal Government and the public and private sector owners and operators of the CIKR, while the President's CPR recommends that the U.S. work with all countries to develop a trusted, safe, and secure cyber infrastructure that enables prosperity for all nations. The *International Strategy for Cyberspace* recommends that the U.S. provide knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity. The strategy also recommends that the U.S. continue to develop and share international cybersecurity best practices with its international partners.

The borderless nature of threats to, and emanating from, cyberspace requires active engagement and strong partnerships with countries around the world. Trust-based working relationships with our international partners are essential in securing the global cyber infrastructure. A number of U.S. Federal entities have responsibilities for, and are involved in, international cyberspace governance and security efforts. Specifically, the Departments of Commerce, Defense, Homeland Security, Justice, and State, among others, are involved in efforts to develop international standards, formulate cyber-defense policy, facilitate overseas investigations and law enforcement, and represent U.S. interests in international forums.

Since the targets of attacks on our critical infrastructure would likely include both government and privately owned facilities, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sectors. Establishing regular communication and personal dialogue with international counterparts will allow U.S. Government agencies to build capacity with other countries and take steps to secure cyberspace collectively. Collaboration among public, private, and international partners enhances information sharing, increases situational awareness, improves incident response capabilities, and supports law enforcement activities.

[51] Public-private partnerships have been defined as collaboration between a public sector (government) entity and a private sector (for-profit) entity to achieve a specific goal or set of objectives. This collaboration results in government-business relationships that include service contracts, supply chains, ad hoc partnerships, and information dissemination partnerships.

Steps for Conducting Cybersecurity-Related Audits

To ensure the continuity and viability of critical infrastructures, all necessary measures should be taken to eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructure and IT systems. Frequent assessments will be made of our critical infrastructures' existing reliability, vulnerability, and threat environment because, as technology and the nature of the threats to our critical infrastructures continue to change rapidly, so must the protective measures and responses.

Proper management of IT systems is essential to ensure the confidentiality, integrity, and availability of critical infrastructure information. Configuration and account access vulnerabilities identified on IT systems must be mitigated to manage and secure the systems and data from the risks associated with internal and external threats, unauthorized access, and misuse. Authorized system administrators, users, and contractor personnel need to be appropriately trained to ensure that data and systems containing the data are adequately safeguarded. Security documentation needs to be updated to ensure that system information is accurate, the appropriate security controls have been evaluated, and the data stored on the system is protected.

The following are audit-specific areas that should be considered when evaluating the security of an agency's critical infrastructure and cyber systems. The steps presented for each audit-specific area provide a baseline for conducting IT security audits and evaluations; they do not include all program steps that can be performed. The types of audits listed are based on audits that have been completed by members within the OIG community:

- Identity Management.
- Network Management and Security.
- Laptop Security.
- Wireless Security.
- Database Security.
- UNIX Operating System Security.
- Remote Access Controls and Security.
- Mobile Device Security.
- Portable Storage Device Security.
- E-mail Security.
- Web Server Security.
- Domain Name System (DNS) Server Security.
- Firewall Security.
- Active Directory (AD) Testing.
- Incident Response, Handling, and Reporting.
- Internet Protocol, Version 6 (IPv6).

- Radio Frequency Identification (RFID) Testing.
- Insider Threats.

Identity Management

The Federal Identity, Credential, and Access Management Initiative efforts, including those of the OIG community, are a key enabler for addressing the Nation's cybersecurity challenges. In recent years, increasing emphasis has also been placed on improving the physical security of the hundreds of thousands of facilities that the Federal Government owns and leases. In addition to complex physical and logical cybersecurity threats, the Federal Government faces significant challenges in carrying out its IT capabilities to enable a level of assurance and electronic service delivery. Standardized controls around identity and access management combine to support an improvement in the cybersecurity posture across the Federal Government.

The Federal Government has long been challenged in employing effective identity management and authentication technologies. In an effort to increase the quality and security of Federal ID and credentialing practices, the President issued HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, in August 2004, requiring the establishment of a government-wide standard for secure and reliable forms of ID.[52] A common, standardized, trusted basis for digital identity and access management is needed to provide a consistent approach to deploying and managing appropriate identity assurance, credentialing, and access control services.

OMB issued Memorandum 5-24 on August 5, 2005. This memorandum provided all departments and agencies with HSPD-12 implementing instructions and guidance, as well as implementation deadlines. Then, in March 2006, NIST issued FIPS 201-1, *Personal Identity Verification of Federal Employees and Contractors*. FIPS 201-1 consists of two parts, PIV-I and PIV-II. The minimum requirements for a Federal personal ID system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance, are described in PIV-I. Detailed technical specifications to support the control and security objectives in PIV-I, as well as the interoperability of PIV cards and systems among Federal departments and agencies, are outlined in PIV-II.

See appendix F for baseline audit objectives and steps that can be used for conducting and evaluating identity management.

[52] The purpose of HSPD-12 is to enhance security, reduce identity fraud, protect personal privacy, and leverage logical (computer) and physical (building access) security through one ID card.

Network Management and Security

Networks are a series of interconnected devices and software that allow individual users and agencies to share information. Since sensitive data is stored on and transmitted along networks, securing networks is essential for protecting sensitive data from unauthorized access, manipulation, and misuse. Adequate network security is needed to protect the confidentiality, integrity, and availability of sensitive information.

A comprehensive approach to network security requires that testing for vulnerabilities be performed from points within the network as well as outside the firewall, and include the testing and verification of network-related security controls (e.g., antivirus software updates, audit trail [system log] monitoring and review process, patch management process) on a regular basis. All points of entry into the network, such as desktop and laptop computers, remote access (Virtual Private Network [VPN] and dial-up), connections to third-party networks, wireless access points, and the network perimeter, must be evaluated. The goal is to eliminate or minimize all security weaknesses and protect the network from both external and internal attack. Routine security testing can prevent many types of security incidents from occurring and uncover unknown vulnerabilities and misconfigurations.

See appendix G for baseline audit objectives and steps that can be used for conducting and evaluating network management and security.

Laptop Security

As the weight and price of laptop computers have decreased and their computing power and ease of use have increased, so has their popularity for use as the primary or only computer for Federal Government employees. The Government is now heavily reliant on laptop computers for conducting its business. The mobility of laptops has increased the productivity of the Federal workforce, but at the same time increased the risk of theft, unauthorized data disclosure, and virus infection. Thefts of laptop computers occur regularly from offices, airports, automobiles, and hotel rooms.

Data on a lost or stolen laptop, if not encrypted, can reveal critical information such as changes to legislation, investigations, or economic analyses. Consequently, government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information that is stored on it are adequately protected. Such steps may include providing additional security awareness training to laptop users, ensuring secure storage of laptop computers when they are not in use, encrypting data files stored on the laptop, and ensuring that adequate security software applications, such as firewalls and antivirus software, are installed and regularly updated.

See appendix H for baseline audit objectives and steps that can be used for conducting and evaluating laptop security.

Wireless Security

The use of wireless networks and devices is becoming increasingly popular throughout the Federal Government environment. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices. The most common communication standards used by wireless devices are the Institute of Electrical and Electronics Engineers (IEEE) 802.11 (802.11x) and Bluetooth. 802.11x devices can form a wireless local area network by connecting through an access point or to other 802.11x devices. Bluetooth is used primarily on handheld devices such as BlackBerries and other smartphones, but can also be used to connect desktop peripherals such as a mouse or keyboard. Two or more Bluetooth devices can form an ad-hoc network by connecting to each other.

Wireless technology can offer Federal agencies many potential benefits in improving employee productivity and flexibility. In addition, wireless network installations can provide tremendous cost savings compared to traditional wired infrastructures. However, wireless networks and devices also present significant security challenges, including protection against outside attacks, physical controls over wireless infrastructure and devices, and unauthorized deployments of wireless networks or access points. In addition, the increased use of wireless technology has introduced several new security risks to the computing environment, including eavesdropping, unauthorized access points, and signal leakage that can compromise sensitive information. As a result, the Federal Government must take the extra effort needed to implement effective security controls necessary to protect sensitive information stored and processed on and by its wireless networks and devices.

See appendix I for baseline audit objectives and steps that can be used for conducting and evaluating the security of wireless networks and devices.

Database Security

A database is one or more large structured sets of data (e.g., fields, records, files) organized so that the data can easily be accessed, managed, and updated. Databases are usually associated with software to update and query the data, called a database management system (DBMS). A DBMS can be an extremely complex set of software programs that control an organization’s storage and retrieval of information in a database. It also controls access to the data and ensures the security and integrity of the database. DBMSs can be classified according to their architectural model (relational, hierarchical, or network) and can be centralized on one platform or distributed across multiple servers.

Databases and DBMSs have become a more frequent target of attack by malicious users. Such an attack can result in financial loss, loss of privacy, a breach of national security, and many other varieties of corruption that can result from unauthorized access to sensitive data. To counter this threat, an increasing number of security options have become available to protect the sensitive data housed in databases. However, for these measures to be effective, DBMS security controls must be properly configured and maintained. In addition, as database products have become more complex and the attacks against them have increased, a number of vulnerabilities have been identified that attackers could exploit. DBMS vendors have responded by issuing patches or fixes for discovered vulnerabilities, but these patches must be quickly and appropriately applied to ensure that sensitive data is adequately protected.

See appendix J for baseline audit objectives and steps that can be used for conducting and evaluating database security.

UNIX Operating System Security

UNIX is a computer operating system that was first developed in 1969 by AT&T employees while at Bell Labs. It was originally conceived as an academic operating system, particularly at the university level, and hence security was not a top design priority. Since then, however, UNIX computing systems have been made more widely available and have become an essential part of networking and Internet infrastructure. Linux, a descendant of UNIX, is a leading operating system on servers and other systems such as mainframe computers and supercomputers; more than 90 percent of today's 500 fastest supercomputers run some variant of Linux. Linux also runs on embedded systems (devices where the operating system is typically built into the firmware and highly tailored to the system) such as mobile phones, tablet computers, network routers, building automation controls, televisions, and video game consoles.

The evolution of UNIX security features continues to this day, with an increasingly urgent need for preventing inappropriate access to systems and their data. The increased level of access and the need for data security have driven improvements to UNIX security features. Whether servers are purchased operating systems with vendor support such as Solaris, Red Hat, or Hewlett-Packard (HP), or an open source Linux variant such as Debian, openSUSE, or Fedora, these servers are all referred to as UNIX servers. Each of these operating systems has unique security vulnerabilities from differing implementations, applications, and services.

See appendix K for a list of audit objectives and steps that can be conducted in evaluating UNIX and Linux operating system security. Depending on the UNIX version being reviewed (which include IBM AIX and Linux), there are STIG templates that can be used to evaluate whether the operating system controls for have been properly implemented. In addition, the CERT Coordination Center (CERT/CC), at Carnegie Mellon University’s Software Engineering Institute, has published a system security checklist that can be used to audit an organization's UNIX network (http://staff.washington.edu/dittrich/R870/security-checklist.html).[53]

Remote Access Controls and Security

Remote access allows trusted computer users to access government networks via modem or the Internet. This allows mobile employees access to network resources (e.g., E-mail messages, files, databases, applications) while they are away from their office. Remote access has numerous advantages; for example, it allows employees who are on travel or telework to access an agency's network and resources.

Though providing government employees with remote access has several advantages, granting and maintaining remote access to government systems and resources also involves numerous security concerns. High-speed Internet access technologies, such as cable modems, fiber-optic lines, satellites, and wireless systems allow for increased transmission speed and bandwidth, and make it easier for users to access and transfer large amounts of data. These factors make remote access users an attractive target for attackers, increasing the risk that malicious users may attempt to gain inappropriate or unauthorized access to government systems and resources from a remote location. Therefore, greater potential exists for the exposure of internal government network resources and data from external sources.

See appendix L for baseline audit objectives and steps that can be used for conducting and evaluating remote access capabilities.

Mobile Device Security

Mobile devices, such as tablets the Android and Apple smartphones, have become widely used tools for today's highly mobile workforce. These devices allow workers to accomplish their duties and carry out their tasks at any time and from any place as well as transport large volumes of data. For example, these devices enable workers to send and receive E-mail messages, browse the Internet, store and modify documents, deliver presentations, and remotely access data.

Mobile devices provide many productivity benefits, but they also expose the organization to new security risks, such as downloading viruses or inadvertently exposing sensitive information or personally identifiable information (PII). In addition, mobile devices, such as tablet computers and smartphones based on Android, Apple iPhone Operating System, Web

[53] CERT/CC studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to help the public improve security. Although it was established as an incident response team, CERT/CC has evolved beyond that, focusing instead on identifying and addressing existing and potential threats, notifying system and other technical personnel of these threats, and coordinating with vendors and incident response teams worldwide to address the threats.

Operating System, and Windows Operating Systems, typically lack several important security features commonly used on desktop computers. Security threats to mobile devices include loss, theft, or disposal; unauthorized access; spam; and electronic eavesdropping and tracking. Further, these devices are difficult to administer centrally because they lack the functionality and security features needed to be easily managed in an enterprise or government environment without employing a third-party application.

See appendix M for baseline audit objectives and steps that can be used for evaluating mobile device security.

Portable Storage Device Security

The proliferation and uncontrolled use of Universal Serial Bus (USB) flash drives and other portable storage devices increase the risk of theft and mishandling of sensitive information. When users insert their personal or unauthorized devices into a computer's USB or FireWire ports to transfer data, new IT security risks can be introduced to agency computers and networks and amplify risks that already exist.[54] Examples of portable storage devices include flash drives, pen drives, external hard drives, and portable music and video players that can also store data (e.g., Apple iPods). These portable devices are small enough to fit into a shirt pocket, relatively inexpensive, and can store a large amount of data.

The risk of unauthorized access to sensitive data becomes more apparent with U3-enabled USB devices.[55] The open-standard U3 platform allows a user to install applications onto the USB drive and then launch them on USB-equipped Windows machines, regardless of whether the user has administrative privileges. A small, 4-megabyte, read-only system partition of the U3 drive looks to the system like a compact disk (CD) read-only memory (ROM) drive, while the data partition looks like a regular flash drive. Windows treats the system partition as a CD. U3 then takes advantage of the AutoPlay feature in Windows to automatically run the U3 LaunchPad application and unlock the data partition of the hard drive. Therefore, unsecured computers might allow these portable devices to install a (1) key catcher program that will capture all characters typed on the computer keyboard, likely including application IDs and passwords; (2) password gathering program that will retrieve Windows password hashes and could later be cracked; (3) vulnerability scanner program that could launch vulnerability scans of devices on the network, obtaining information that could later be used to gain unauthorized access; or (4) virus that could propagate across the network, affecting system availability.

---

[54] The IEEE 1394 interface, developed in the late 1980s and early 1990s by Apple as FireWire, is a serial bus interface standard for high-speed communications and isochronous real-time data transfer. This interface is comparable with USB, and often those two technologies are considered together.

[55] U3 was a joint venture that produced a proprietary method of launching Windows applications from special USB flash drives.

See appendix N for baseline audit objectives and steps that can be used for conducting and evaluating portable storage device security.

E-mail Security

E-mail is the most popularly used system for exchanging information over the Internet, and is a critical tool used by government agencies to complete their missions. Sensitive data is often sent via E-mail within an agency as well as between government employees and outside entities. In today's network environment, E-mail is also a preferred path hackers use to distribute viruses, worms, spam, and other attacks. E-mail system servers are among the most targeted and attacked machines within an organization's network, second only to web servers. It is critical to protect information sent or received via E-mail from unauthorized use, disclosure, modification, destruction, or exploitation.

See appendix O for baseline audit objectives and steps that can be used for conducting and evaluating E-mail security.

Web Server Security

The World Wide Web is a system for exchanging information over the Internet. At the most basic level, it can be divided into two principal components: (1) web servers that make information available over the Internet (in essence, provide hosting services), and (2) websites and applications using software to access and display the information stored on web servers and support systems.

An agency's public-facing website is the most accessible point of entry and attack to its resources.[56] These types of sites and the servers that support them are useful in providing information and services, but they are often the most targeted and attacked hosts on organizations' networks. Web servers and the network infrastructure that supports them must be configured to protect sensitive data.

Appropriate management practices are essential to operating and maintaining a secure web server. Security practices entail the ID of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources.

[56] A public-facing website is a website freely accessible by all Internet users. Typically, it contains information about an organization's business, products, services, contact information, and history. It may also have links to other related websites. It is an information source about an organization for its customers and partners.

See appendix P for baseline audit objectives and steps that can be used for conducting and evaluating web server security.

DNS Server Security

An IP address is a numerical label assigned to each device (e.g., computer, printer) configured on a computer network that uses the IP for communication. Computers in the network route communication packets across the Internet based on the IP addresses of the packets. However, when accessing websites and using E-mail services, a user can simply employ a domain name, such as DHS.gov or DOJ.gov that is easier to remember than a full IP address. The DNS transforms human-readable domain names into machine-readable IP addresses and also does the reverse process, taking a query with an IP address and returning the associated domain name.

The primary security goals for DNS are data integrity and source authentication, both needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit. DNS services and data availability are also important; DNS components are often subjected to denial-of-service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. DNS deployments must be configured to prevent denial-of-service attacks that exploit vulnerabilities in various DNS components. DNS is susceptible to the same types of vulnerabilities (platform, software, and network level) as any other distributed computing system.

As part of the Federal Government's effort to increase its level of service to the public, agencies have been instructed to implement Domain Name System Security (DNSSEC) extension measures to all websites in the ".gov" domain. The purpose of this initiative is to ensure that public users of government services who are provided online access are confident that a website they visit and over which they transmit information is an authentic government website and secure. Securing Federal Internet domains is of critical importance given the government's increased reliance on the Internet to provide services and disseminate information to the public. OMB Memorandum 08-23 establishes authority to secure the Federal Government's DNS Infrastructure.

See appendix Q for baseline audit objectives and steps that can be used for conducting and evaluating the management and security measures in place over DNS servers.

Firewall Security

Network firewalls protect systems and networks from external threats.[57] Firewalls can block access to internal services, bar unwanted users, and in some cases, filter network traffic by content. However, hackers utilize several exploits to penetrate firewalls and undermine firewall security. The most common of these include brute force, backdoor passwords, service provider passwords, improper configuration, firmware bugs, and telnet/web access. Firewall audits can evaluate the security posture of a network. Beyond compliance requirements, firewall audits can increase the chances of catching weaknesses in an organization's network and identify deficiencies in firewall policies that need to be addressed. Two of the most important aspects of conducting a firewall audit are to review the change process and the firewall rule base (also called a policy).

See appendix R for baseline audit objectives and steps that can be used for conducting and evaluating firewall security controls. In addition, the SANS Institute has developed a firewall checklist as part of its Security Consensus Operational Readiness Evaluation program that can be used to audit a firewall. The checklist does not provide vendor-specific security considerations, but rather attempts to provide a generic listing of security considerations to be used when auditing a firewall (http://www.sans.org/score/checklists/FirewallChecklist.pdf).

AD Testing

AD is the directory service associated with Microsoft® Windows Server operating systems. It enables centralized, secure management of an entire network of users and acts as a data store for multiple kinds of enterprise information. AD also allows administrators to add, delete, organize, and maintain user, local administrative, and system service accounts, as well as define group policy objects to enforce password and permission polices across an enterprise.

The distributed nature of an organization's component networks requires the use of many trusts between their AD servers. These trusts, the process for allowing a user to authenticate to one domain and access resources in another domain without authenticating again, must be secured and maintained to protect the organization's data and services. Trust zones within and throughout these networks pose a significant security risk if they are not effectively configured, implemented, and managed.

Because AD is such a powerful tool for administrators, access should be limited to minimize the threat of insider attacks—either malicious or a result of human error—as well as external attacks that could elevate privileges through weak security measures. Attacks on networks could be successful via faulty trust authentication, unpatched domain controllers, or

[57] Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.

unstructured system and management policies that do not separate duties and enforce least privilege. Such attacks could result in unauthorized access to an organization's data or resources.

Effective access controls implemented through AD services and trusts are a core element of an enterprise security program. Additionally, the overall security posture must include elements such as group policy objects in place to enforce password and file permissions, administrative efforts and policy enforcement for inactive account removal, event logging, and up-to-date patches on domain controllers.

See appendix S for baseline audit objectives and steps that can be used to test and evaluate AD controls.

Incident Response, Handling, and Reporting

Computer security incident response has become an important component of IT programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring threats through IDSs and other mechanisms is essential. The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. Therefore, establishing clear procedures for assessing the current and potential business effect of incidents is crucial, as is implementing effective methods of collecting, analyzing, and reporting data. Also, building relationships and developing a means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are vital for an organization's incident response and reporting system.

See appendix T for baseline audit objectives and steps that can be used for conducting and evaluating an agency's incident response, handling, and reporting capabilities.

IPv6

IP is the common language that allows different types of information, such as E-mail and other data, voice communications, and video, to travel seamlessly over the same network or the

Internet. Many devices that connect to the Internet need a unique IP address. IP addresses identify information's origin and destination.

The existing protocol supporting the Internet today is Internet Protocol, Version 4 (IPv4), which defines an IP address as a 32-bit number. However, IPv4 provides only 4 billion IP addresses, inherently limiting the number of devices that can have a unique, globally routable location on the Internet. Due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), introduced as the next generation of IP using a 128-bit address, was developed in 1995. IPv6 was standardized in 1998, and its deployment has continued since the mid-2000s.

IPv6 provides more addresses and many features to enhance the use and efficiency of networking. It provides an exponentially larger number of available IP addresses and is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity. Federal agencies must prepare for the future of networking and Internet technology by enabling their networks to support IPv6 addresses and data packets.

See appendix U for baseline audit objectives and steps that can be used for conducting and evaluating an agency's implementation of IPv6.

RFID Testing

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a device called an RFID tag. The technology provides a more efficient method for Federal agencies, manufacturers, retailers, and suppliers to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls by providing real-time access to information. Technology components of an RFID system consist of a tag, reader, and database.

Adequate security controls are needed to protect the confidentiality, integrity, and availability of the information contained on RFID tags and in the database systems where information is stored and retrieved. Privacy concerns must also be addressed when implementing a system using RFID technology. The primary reason for developing controls and testing the security of RFID is to identify potential issues and vulnerabilities and put preventive and detective controls into place. Since this is a relatively new technology for the Federal Government, there is little guidance and policy governing RFID technology or controls.

See appendix V for baseline audit objectives and steps that can be used for evaluating and testing RFID controls.

Insider Threats

Insider threats represent the greatest risk to computer security because an organization's own employees understand how the computer systems work. According to Gartner, Inc., more than 70 percent of data thefts, data breaches, and instances of unauthorized access to data are committed by an organization's own employees.[58] Effectively mitigating the insider threat requires policies, practices, and continued training.

Two common policy areas that can reduce insider threat are access controls and segregation of duties. Poor access controls enable an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. Segregation of duties is important in ensuring the integrity of an enterprises information system. No one individual should have complete control of any system. Failing to properly segregate the computer duties of an organization's staff can dramatically increase the risk of errors or fraud.

Monitoring users' access and data actions on a system is not enough. Once the enterprise develops a policy and presents it to all users, it must enforce the policy. Software and hardware solutions currently allow the input of policy in human terms, translate it to machine code, and then monitor at the packet level of all data transactions within, and outbound from, the network. Packet monitoring for policy compliance is one way to enforce the policy itself. Without this approach, the administrator is dependent on the trustworthiness of the users to adhere to the policy.

See appendix W for baseline audit objectives and steps that can be used for conducting and evaluating insider threats.

[58] Gartner, Inc. is a world leading IT research and advisory company.

Appendix A
Additional References to Relevant Requirements and Guidance

Executive Order 13286
This order, issued in February 2003, specifies the national policy statement regarding the protection against disruption of information systems for critical infrastructures. The order designates the National Infrastructure Advisory Council to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy through the Secretary of Homeland Security.
(http://www.fas.org/irp/offdocs/eo/eo-13286.htm)

Freedom of Information Act
Enacted on July 4, 1966, and taking effect one year later, the Freedom of Information Act provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure. Under the Act, agencies must disclose any information that is requested, unless that information is protected from public disclosure. It also requires that agencies automatically disclose certain information, including frequently requested records.

The Freedom of Information Act is a law that gives individuals the right to access information from the Federal Government. It is often described as the law that keeps citizens in the know about their government.
(http://www.foia.gov/)

PDD-63
PDD-63, Critical Infrastructure Protection, issued in May 1998, required the establishment of lead agencies for infrastructure sectors that could become targets for significant cyber or physical attacks. As required by PDD-63, the Federal Government and private sectors were to produce a National Infrastructure Assurance Plan that, among other initiatives, included:

- Performance of initial vulnerability assessments, followed by periodic updates, for each sector of the economy and government that might become a target of an infrastructure attack intended to significantly damage the U.S.

- Development and implementation of a remedial plan, based upon the results of the vulnerability assessments, to identify timelines, responsibilities, and funding for addressing identified risks.

On December 17, 2003, PDD-63 was superseded by HSPD-7. HSPD-7 required Federal departments and agencies to identify and prioritize the Nation's critical infrastructures and key resources and to protect them from terrorist attacks. In February 2013, PDD-21 revoked

HSPD-7. Under PDD-21, critical infrastructure security and resilience is to be a shared responsibility among Federal, State, local, tribal and territorial entities, and public and private owners and operators of critical infrastructure.
(http://www.fas.org/irp/offdocs/pdd/pdd-63.htm)

HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors
Traditionally, a wide range of procedures has been employed to authenticate an individual's identity, using various classes of credentials for both physical access to buildings and authorization to access computers and data. HSPD-12, signed in 2004, established a mandatory government standard for secure and reliable ID credentials issued by government departments and agencies to its employees and contractors. The policy is intended to enhance security, increase efficiency, reduce identify fraud, and protect personal privacy. These credentials are to be used for gaining physical and logical access to federally controlled facilities and information systems.
(http://www.dhs.gov/homeland-security-presidential-directive-12)

Homeland Security Act of 2002
In November 2002, this act created DHS, with the overriding mission of protecting the U.S. from further terrorist attacks. Under the act, DHS was assigned the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the U.S.; (2) recommending measures to protect the key resources and critical infrastructures of the U.S. in coordination with other groups; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks.
(http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf)

The National Strategy for Homeland Security
In response to the terrorist attacks that occurred in September 2001, *The National Strategy for Homeland Security*, issued in July 2002, was developed to mobilize and organize the Nation to secure the U.S. from terrorist attacks. The strategy identified eight major initiatives, including the need to secure cyberspace and unify the Nation's infrastructure protection efforts in DHS.
(http://www.ncs.gov/library/policy_docs/nat_strat_hls.pdf)

National Response Framework
The U.S. National Response Framework is part of *The National Strategy for Homeland Security*, which presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies, from the smallest incident to the largest catastrophe. It establishes a comprehensive, national, all-hazards approach to domestic incident response.
(http://www.fema.gov/national-response-framework)

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
Issued in February 2003, this strategy provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. This strategy builds on the sector-based approach of PDD 63 and calls for expanding the capabilities of information sharing and analysis centers. The strategy describes three key objectives: (1) identifying and ensuring the protection of the most critical assets, systems, and functions; (2) ensuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to ensure the protection of other potential targets. (http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf)

Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (Version 1.0)
In November 2009, the Federal Chief Information Officers Council issued this document to present the Federal Government with a common framework and implementation guidance needed to plan and execute ID, credential, and access management programs. Standardized identity and access management controls combine to support an improvement in the cybersecurity posture across the Federal Government. (http://www.idmanagement.gov/documents/ficam_roadmap_implementation_guidance.pdf)

NIST SP 500-267 – *A Profile for IPv6 in the U.S. Government Version 1.0*
NIST SP 500-267, issued in July 2008, defines a standards profile for IPv6 in the U.S. Government that is intended to be applicable to all future uses of IPv6 in non-classified, non-national security Federal IT systems. The standards profile is meant to (1) define a simple catalog of common network devices; (2) define the minimal mandatory IPv6 capabilities and identify significant configuration options to assist agencies in the development of more specific acquisition and deployment plans; and (3) provide the technical basis upon which future U.S. Government policies can be defined. (http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf)

NIST SP 800-40 – *Creating a Patch and Vulnerability Management Program* (Version 2.0)
Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of IT systems. In November 2005, this document was issued to provide basic guidance for establishing a patch and vulnerability management program and testing the effectiveness of that program. It also provides technical solutions that are available for vulnerability remediation. (http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf)

NIST SP 800-40 – *Guide to Enterprise Patch Management Technologies* (Revision 3)
This publication, issued in July 2013, is designed to assist organizations in understanding the basics of enterprise patch management technologies. The information contained in this

publication assumes that the organization has a mature patch management capability and is focused on increasing its automation level.[59] It was developed for security managers, engineers, administrators, and others responsible for acquiring, testing, prioritizing, implementing, and verifying security patches. In addition, this publication may be used by auditors in assessing the security of systems. It covers the importance of patch management, the challenges of patch management, enterprise patch management technologies, and metrics. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf)

NIST SP 800-41 – *Guidelines on Firewalls and Firewall Policy* (Revision 1)
NIST SP 800-41, issued in September 2009, describes the capabilities of firewall technologies and firewall policies. It also provides practical guidance on developing firewall policies and selecting, configuring, testing, deploying, and managing firewalls. (http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf)

NIST SP 800-44 – *Guidelines on Securing Public Web Servers* (Version 2)
Issued in September 2007, this guide recommends security practices for designing, implementing, and operating publicly accessible web servers, including related network infrastructure issues. This document can be used by organizations interested in enhancing security on existing and future web server systems to reduce the number and frequency of web-related security incidents. (http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf)

NIST SP 800-45 – *Guidelines on Electronic Mail Security* (Version 2)
Attackers frequently target mail servers. Various types of email content and attachments have also proven to be effective in introducing viruses and other malware into networks through mail clients. Email is extensively used to deliver attacks that exploit vulnerabilities in users' workstations or use social engineering methods to trick users. These attacks often lead to the compromise of the user workstation or the release of sensitive information even when the email client is securely configured. This document, issued in February 2007, recommends security practices for designing, implementing, and operating E-mail systems on public and private networks. (http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf)

NIST SP 800-46 – *Guide to Enterprise Telework and Remote Access Security* (Revision 1)
This guide, issued in June 2009, was developed to assist organizations in mitigating the risks associated with the enterprise technologies used for telework, including remote access servers, telework client devices, and remote access communications. The document emphasizes the importance of securing sensitive information stored on telework devices and transmitted

[59] Organizations seeking more basic guidance on establishing a patch management program or that that have legacy needs that cannot be met with current enterprise management technologies could consult the previous complementary publication, NIST SP 800-40 (Version 2), *Creating a Patch and Vulnerability Management Program*.

through remote access across external networks. It also provides recommendations for creating telework-related policies and for selecting, implementing, and maintaining the necessary security controls for remote access servers and clients.
(http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf)

NIST SP 800-48 – *Guide to Securing Legacy IEEE 802.11 Wireless Networks* (Revision 1)
Wireless local area networks (WLAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication. WLANs are usually implemented as extensions to existing WLANs to provide enhanced user mobility and network access. The most widely implemented WLAN technologies are based on IEEE 802.11 and its amendments. This document, issued in July 2008, is to provide guidance to organizations in securing their legacy IEEE 802.11 WLANs that cannot use IEEE 802.11i.
(http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf)

NIST SP 800-63 – *Electronic Authentication Guideline* (Version 1.0.2)
This document, issued in December 2011, provides technical guidance to Federal agencies implementing electronic authentication (e-authentication).[60] It covers remote authentication of users over open networks and defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols, and related assertions.
(http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf)

NIST SP 800-70 – *National Checklist Program for IT Products - Guidelines for Checklist Users and Developers* (Revision 2)
In February 2011, NIST SP 800-70 was issued to describe security configuration checklists and their benefits, and explain how to use the NIST National Checklist Program to find and retrieve checklists. Prepared for use by Federal agencies, the document also describes the policies, procedures, and general requirements for participation in the NIST Checklist Program.
(http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf)

NIST SP 800-73-3 – *Interfaces for Personal Identity Verification* (4 Parts)
HSPD-12 required the adoption of a common ID standard to govern the interoperable use of identity credentials for physical and logical access to Federal Government locations and systems. This document, issued in February 2010, contains technical specifications to interface, retrieve, and use identity credentials, and is a companion document to FIPS-201. FIPS 201 was developed to establish standards for identity credentials.
(http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf)

[60] E-authentication is the process of establishing confidence in user identities electronically presented to an information system.

(http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART2_piv-card-applic-card-common-interface.pdf)
(http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART3_piv-client-applic-programming-interface.pdf)
(http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART4_piv-transitional-interface-data-model-spec.pdf)

NIST SP 800-76-1 – *Biometric Data Specification for Personal Identity Verification*
This publication, issued in January 2007, is a companion document to FIPS 201. It contains technical specifications for biometric data mandated in FIPS. These specifications reflect the design goals of universal interoperability and high performance of the PIV card.[61] The specifications also address image acquisition to support background check, fingerprint template creation, retention, and authentication.
(http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf)

NIST SP 800-79-1 – *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*
HSPD-12 mandates that PIV cards be "issued only by providers whose reliability has been established by an official accreditation process." This document, issued in June 2008, contains guidelines for satisfying the requirements for an official accreditation and provides a methodology that any organization can utilize to formally accredit a PIV Card Issuer (PCI). This methodology consists of two major elements–assessment[62] and accreditation.[63] This document is applicable to, and shall be used by, all Federal organizations for all their employees and contractors for authorizing their physical access to Federal facilities (e.g., buildings, leased offices) and logical access to Federal information systems.
(http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf)

NIST SP 800-81 – *Secure Domain Name System (DNS) Deployment Guide* (Revision 1)
NIST issued SP 800-81 in April 2010 to provide deployment guidelines for securing DNS within an enterprise.[64] The DNS infrastructure is made up of computing and communication entities that are geographically distributed throughout the world. Because DNS data is meant to be public, preserving the confidentiality of DNS data pertaining to publicly accessible IT resources

[61] A PIV card is a physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, biometric data) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
[62] Assessment, which occurs before accreditation, is the process of gathering evidence regarding a PCI's satisfaction of the requirements of FIPS 201-1, both at the organization and facility level.
[63] Accreditation is the decision to authorize the operation of a PCI once it has been established that the requirements of FIPS 201-1 have been met and the risks regarding security and privacy are acceptable.
[64] To access Internet resources by user-friendly domain names rather than IP addresses, users need a system that translates domain names to IP addresses and back. This translation is the primary task of an engine called the DNS.

is not a concern. The primary security goals for DNS are data integrity and source authentication, both needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit.

This document provides extensive guidance on maintaining data integrity and performing source authentication. Availability of DNS services and data is also important; DNS components are often subjected to denial-of-service attacks intended to disrupt access to the resources whose domain names are handled by the attacked DNS components. This document outlines the guidelines for configuring DNS deployments to prevent many denial-of-service attacks that exploit vulnerabilities in various DNS components.
(http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf)

NIST SP 800-82 – *Guide to Industrial Control Systems Security*
Control systems are vital to the operation of the U.S. critical infrastructures, which are often highly interconnected and mutually dependent systems. This document provides guidance for establishing secure ICSs that include supervisory control and data acquisition systems, distributed control systems, and other control system configurations. ICSs are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, durable goods). Supervisory control and data acquisition systems are generally used to control dispersed assets using centralized data acquisition and supervisory control, while distributed control systems are generally used to control production systems within a local area. This guide was issued in June 2011 to provide an overview of ICSs and typical system topologies, identify typical threats and vulnerabilities to these systems, and provide recommended security countermeasures to mitigate the associated risks.
(http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)

NIST SP 800-92 – *Guide to Computer Security Log Management*
A log is a record of the events occurring within an organization’s systems and networks. Logs are composed of entries that contain information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and IDPSs; operating systems on servers, workstations, and networking equipment; and applications.

This guide was issued in September 2006 to provide guidance for developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization.
(http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf)

NIST SP 800-95 – *Guide to Secure Web Services*
The security challenges presented by the web services approach are formidable and unavoidable. This publication, issued in August 2007, provides practical, real-world guidance on current and emerging standards applicable to web services, as well as background information on the most common security threats to service-oriented architectures based on web services. This document presents information that is largely independent of particular hardware platforms, operating systems, and applications.
(http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf)

NIST SP 800-97 – *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
One of the most active standards organizations that address wireless networking is the IEEE. This publication, issued in February 2007, seeks to assist organizations in understanding, selecting, and implementing technologies based on IEEE 802.11i, part of the IEEE 802.11 family of wireless networking standards. Through its framework for security networks, this document explains the security features and capabilities associated with IEEE 802.11i, and provides extensive guidance on the planning and deployment of robust security networks.
(http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf)

NIST SP 800-111 – *Guide to Storage Encryption Technologies for End User Devices*
In today's computing environment, there are many threats to the confidentiality of information stored on end user devices. This guide, issued in November 2007, outlines storage encryption technologies for end user devices and for planning, implementing, and maintaining storage encryption solutions. The types of end user devices it addresses are personal computers (e.g., desktops, laptops), consumer devices (e.g., personal digital assistants, smartphones), and removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs, digital video disks).
(http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf)

NIST SP 800-115 – *Technical Guide to Information Security Testing and Assessment*
An information security assessment is the process of determining how effectively an entity (e.g., host, system, network, procedure, person—known as the assessment object) meets specific security objectives. This document, issued in September 2008, is a guide to the basic technical aspects of conducting information security assessments. It presents technical testing and examination methods and techniques that an organization might use as part of an assessment, and offers insights to assessors on their execution and the impact they may have on systems and networks.
(http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)

NIST SP 800-119 – *Guidelines for the Secure Deployment of IPv6* (December 2010)
The migration to IPv6 services is inevitable, as the IPv4 address space is almost exhausted. IPv6 is not backward compatible with IPv4, which means that organizations will have to change their network infrastructure and systems to deploy IPv6. This document provides guidelines for

organizations to aid in securely deploying IPv6. Since the majority of organizations will most likely run both IPv6 and IPv4 on their networks for the foreseeable future, this document speaks about the deployment of IPv6 rather than the transition to IPv6.

Federal agencies will most likely face security challenges throughout the deployment process, including:

- An attacker community that is likely to have more experience and comfort with IPv6 than an organization in the early stages of deployment.
- Difficulty in detecting unknown or unauthorized IPv6 assets on existing IPv4 production networks.
- Added complexity while operating IPv4 and IPv6 in parallel.
- Lack of IPv6 maturity in security products when compared to IPv4 capabilities.
- Proliferation of transition-driven IPv6 (or IPv4) tunnels, which complicate defenses at network boundaries even if properly authorized, and can completely circumvent those defenses if unauthorized (e.g., host-based tunnels initiated by end users).

(http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf)

NIST SP 800-120 – *Recommendation for EAP Methods Used in Wireless Network Access Authentication*

As different wireless technologies are launched to enable user mobility and provide pervasive network and service accessibility, security has been a prominent requirement for the Federal Government in such access environments. Access authentication and the establishment of keys that protect wireless traffic are both core security components in wireless applications. The Extensible Authentication Protocol (EAP) is a framework for access authentication that supports different authentication methods. Currently, EAP various wireless standards have adopted EAP as an access authentication and key establishment protocol. It is desirable for EAP methods used for WLAN to support mutual authentication and key derivation.

This recommendation, issued in September 2009, formalizes a set of core security requirements for EAP methods when employed by the Federal Government for wireless access authentication and key establishment. The requirements should be considered generic, in the sense that they are independent of specific wireless technologies.
(http://csrc.nist.gov/publications/nistpubs/800-120/sp800-120.pdf)

NIST SP 800-121 – *Guide to Bluetooth Security* (Revision 1)

Bluetooth is an open standard for short-range radio frequency communication. Bluetooth technology is used primarily to establish wireless personal area networks, commonly referred to as ad hoc or peer-to-peer networks. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial-of-service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that

target known vulnerabilities in Bluetooth implementations and specifications. Issued in June 2012, this guide provides information to organizations on the security capabilities of Bluetooth and provide recommendations to organizations employing Bluetooth technologies on securing them effectively.
(http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf)

NIST SP 800-123 – *Guide to General Server Security*
An organization's servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. Some of the most common types of servers are web, email, database, infrastructure management, and file servers. This publication addresses the general security issues of typical servers—the fundamental activities performed as part of securing and maintaining the security of servers that provide services over network communications as a main function. Issued in July 2008, this document addresses common servers that use general operating systems such as Unix, Linux, and Windows.
(http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf)

NIST SP 800-124 – *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (Revision 1 - Draft)
Mobile devices, such as smartphones and tablets, typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. The purpose of this publication, issued in draft in June 2013, is to help organizations centrally manage and secure mobile devices against a variety of threats. It provides recommendations for selecting, implementing and using centralized management technologies and explains the security concerns inherent in mobile device use. The scope covers both organization-provided and personally-owned (bring your own device) mobile devices. Laptops and mobile devices with minimal computing capabilities, such as basic cell phones, are not included within the scope of this publication.
(http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf)

NIST SP 800-144 –*Guidelines on Security and Privacy in Public Cloud Computing*
Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services. Cloud computing is to enable these resources to be rapidly provisioned and released with minimal management effort or cloud provider interaction. In public clouds, however, the infrastructure and computational resources are owned and operated by an outside party that delivers services to the general public via a multi-tenant platform.

This publication, issued in December 2011, provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud

environment. It also describes the threats, technology risks, and safeguards surrounding public cloud environments, and their treatment.
(http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf)

OMB Circular A-130 (Revised – Management of Federal Information Resources
This circular, last updated in 2000, establishes policy for the management of Federal information resources government-wide. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices. The policies in this circular apply to the information activities of all agencies of the executive branch of the Federal Government. The Director of OMB will use IT planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this circular.
(http://www.whitehouse.gov/omb/circulars_a130_a130trans4#1)

OMB Memorandum 05-22 – *Transition Planning for Internet Protocol Version 6 (IPv6)*
This memorandum and its attachments provide guidance to Federal agencies to ensure an orderly and secure transition from IPv4 to IPv6. It required all Federal agency network infrastructures use IPv6 by June 2008. The memorandum includes milestones outlining goals and dates to transition to IPv6.
(http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf)

OMB Memorandum 05-24 – *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
On August 27, 2004, the President signed HSPD-12. The directive requires agencies to develop and implement a mandatory, government-wide standard for secure and reliable forms of ID for Federal employees and contractors. As required by the directive, the Department of Commerce issued FIPS 201. This memorandum provides implementing instructions for HSPD-12 and FIPS 201.
(http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf)

OMB Memorandum 06-06 – *Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12*
OMB guidance itemizes the privacy-related elements of HSPD-12 implementation based on existing requirements to inform individuals about collections of their personal information. Included as attachments to this memorandum are sample privacy documents (e.g., Privacy Act systems of records notices, Privacy Act statements, and a privacy impact assessment) to use as models in implementing HSPD-12 at Federal agencies.
(http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-06.pdf)

OMB Memorandum 06-16 – *Protection of Sensitive Agency Information*
In addition to NIST's checklist for protection of remote information, this memorandum recommends that all departments and agencies take actions including (1) encrypting all data on mobile computers/devices that carry agency data unless the data are determined to be nonsensitive; (2) allowing remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; (3) using a "timeout" function for remote access and mobile devices, requiring user reauthentication after 30 minutes of inactivity; and (4) logging all computer-readable data extracts from databases holding sensitive information and verifying that each extract including sensitive data has been erased within 90 days or that its use is still required.
(http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf)

OMB Memorandum 06-18 – *Acquisition of Products and Services for Implementation of HSPD-12*
This memorandum provides updated direction for the acquisition of products and services for the implementation of HSPD-12 and also provides status of implementation efforts.
(http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2006/m06-18.pdf)

OMB Memorandum 06-19 – *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
This memorandum provides updated guidance on the reporting of security incidents involving PII and explains new requirements that need to be provided in agency budget submissions for IT.
(http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf)

OMB Memorandum 07-06 – *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*
This memorandum discusses validation and monitoring of agency issuance of PIV-compliant identity credentials. It also specifies the requirements for agencies to complete background checks on all current employees and contractors, and the issuance of PIV credentials according to the technical specifications documented in FIPS 201.
(http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-06.pdf)

OMB Memorandum 08-23 – *Securing the Federal Government's Domain Name System Infrastructure*
This memorandum, issued in August 2008, describes existing and new policies for deploying DNSSEC to all Federal information systems. DNSSEC provides cryptographic protections to DNS communication exchanges, thereby removing threats of DNS-based attacks and improving the overall integrity and authenticity of information processed over the Internet.
(http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-23.pdf)

FIPS 112 – *Password Usage*
A password is a sequence of characters that can be used for several authentication purposes. This standard identifies fundamental automated data processing management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features that may be implemented in an automated data processing system in order to support a password system. Those technical features desired by the automated data processing management should be specified in all procurement documents when acquiring new systems and provisions should be made to ensure that they are included when upgrading existing systems.
(http://www.itl.nist.gov/fipspubs/fip112.htm)

FIPS Publication 140-2 – *Security Requirements for Cryptographic Modules*
The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard that Federal organizations will use to specify that cryptographic-based security systems are to be used to protect sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.[65]
(http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

FIPS Publication 197 – *Advanced Encryption Standard (AES)*
The AES specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into their original form, called plaintext.
(http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

FIPS Publication 199 – *Standards for Security Categorization of Federal Information and Information Systems*
This publication addresses standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal Government, promotes (1) effective management and oversight of information security programs, including

[65] A cryptographic module is the set of hardware, software, and/or firmware that implements FIPS-approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. The cryptographic boundary is an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (2) consistent reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
(http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

FIPS Publication 200 – *Minimum Security Requirements for Federal Information and Information Systems*
FIPS Publication 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal Government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. This standard promotes the development, implementation, and operation of more secure information systems within the Federal Government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.
(http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf)

FIPS Publication 201-1 – *Personal Identity Verification of Federal Employees and Contractors* (with Change Notice 1)
This standard, issued in March 2006, specifies the architecture and technical requirements for a common ID standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.
(http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf)

Federal Information System Controls Audit Manual (FISCAM) (Revised)
FISCAM presents a methodology for performing information system control audits of Federal and other government entities in accordance with generally accepted government auditing standards, where system controls are significant to the audit objectives. Developed by GAO with significant CIGIE input and revised in February 2009, this manual focuses on evaluating the effectiveness of general and application controls.
(http://www.gao.gov/assets/80/77142.pdf)

Guide to Securing Microsoft® Windows 2000 Active Directory
Developed by NSA, this draft document provides AD security configuration guidance and recommendations. AD is the directory service used for Windows 2000 domain controllers. According to Microsoft, a directory is a source used to store information about objects, and a directory service includes both the information source and the services making the information available to users. In its simplest definition, AD is a hierarchical namespace of objects that is

tightly integrated with the DNS. AD holds information on objects stored in underlying domains and provides a method for safeguarding directory objects from unauthorized access. (http://www.nsa.gov/ia/_files/os/win2k/w2k_active_dir.pdf)

Microsoft's *Best Practice Guide for Securing Active Directory Installations*
This guide contains recommendations for protecting domain controllers against known threats, establishing administrative policies and practices to maintain network security, and protecting DNS servers from unauthorized updates. It also provides guidelines for maintaining AD security boundaries and securing AD administration, and procedures for enacting the recommendations. The scope of this guide is limited to recommendations for deploying and securing AD domain controllers.
(http://technet.microsoft.com/en-us/library/cc773365(v=ws.10).aspx)

Microsoft's *Exchange Server 2003 Security Hardening Guide*
This guide is designed to provide essential information about how to harden an organization's Microsoft Exchange Server 2003 environment. In addition to practical, hands-on configuration recommendations, this guide includes strategies for combating spam, viruses, and other external threats to the Exchange 2003 messaging system.
(http://technet.microsoft.com/en-us/library/aa997203(v=exchg.65).aspx)

***CIS Exchange Server 2003 Benchmark* (Version 1.0)**
This CIS document provides security configuration guidance for Microsoft Exchange Server 2003. The CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere as a public service to Internet users worldwide. Recommendations result from a consensus-building process that involves many security experts and are generally generic in nature.
(http://www.nsa.gov/ia/_files/vtechrep/I333-TR-999-2005.pdf)

Federal Identity Management Handbook (version 0.1)
In December 2005, the General Services Administration issued this handbook as an implementation guide for government agency credentialing managers, their leadership, and other stakeholders in pursuing compliance with HSPD-12 and FIPS 201. While this handbook cites policies and standards, it is not a policy document. It is intended as a resource for agency implementers of HSPD-12.
(http://www.hss.doe.gov/HSPD12/ficc/FederalIdentityManagementHandbook.pdf)

INCITS 256-2007 – RFID
This standard, developed by the American National Standards Institute (ANSI), establishes a technical standard for a family of compatible RFID devices, specifically RFID devices operating in freely available international frequency bands at license-free power levels.[66]
(http://www.webstore.ansi.org/RecordDetail.aspx?sku=ANSI+INCITS+256-2007)

ISO/IEC 18000-1 – Radio Frequency Identification for Item Management (Revised)
Given the growing use of RFID, from supply chain management to tracking packages to locating and identifying luggage, the International Organization for Standardization (ISO)[67] and the International Electrotechnical Commission (IEC) issued this revised standard to address RFID for item management.[68] This document provides definitions for the generic architecture concepts that commonly require item ID within the logistics and supply chain. It also guides the parameters that are needed in any standardized air interface definition—the communication that occurs between the RFID tag or device and the RFID reader. In addition, the document provides parameter definitions for communications protocols within a common framework for internationally usable frequencies for RFID, as well as reference information regarding relevant patents.
(http://www.iso.org/iso/catalogue_detail?csnumber=46145)

Recommendation ITU-T X.1500 – Cybersecurity Information Exchange Techniques (Draft)
This International Telecommunication Union (ITU) recommendation describes techniques for exchanging cybersecurity information.[69] These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely, and assured information exchange.
(http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11060)

[66] The ANSI oversees the creation, promulgation, and use of thousands of norms and guidelines that directly affect businesses in nearly every sector, from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more.
[67] The ISO is the world's largest developer of voluntary international standards for products, services, and good practice, helping to make industry more efficient and effective.
[68] The IEC is the world's leading organization that prepares and publishes international standards for all electrical, electronic, and related technologies.
[69] The ITU is the United Nations specialized agency for telecommunications, information, and communications technologies. The ITU-T is responsible for studying technical, operating, and tariff questions and issuing recommendations on them with a view of standardizing telecommunications on a worldwide basis.

Appendix B
2013 and Beyond Threat Landscape

Today, cybersecurity is more than detecting a virus or worm. Today's world of cybersecurity consists of not only detecting complicated malware, but also detecting adversaries – insider and outsiders – determining what data left the organization, developing defensive and preemptive measures to keep the attacks from happening in the first place, and most importantly, managing risk-based compliance.

Every attack on an organization begins with a single vulnerability – usually a hole in an application, an open port on a network, or a misconfigured device. Protecting data in a world where systems are changing rapidly, and information flows freely, requires a coordinated effort to secure these systems at the endpoint and gateway, on mobile devices, and in the cloud. Cyber criminals are increasingly using advanced methods to implement attack techniques (vectors) that are non-traceable and difficult to take down. The widespread use of mobile devices leads to an amplification of abuse based on knowledge/attack methods targeting social media; outages in telecommunications infrastructures impact a considerable number of users. The availability of malware and cyber hacking tools and services, together with digital currencies (e.g., Bitcoins) and anonymous payment services, is opening up new avenues for cyber fraud and criminal activity.

Based on a number of industry research reports, below are the top types or "classes" of system and cyber security threats with major impact for 2013 and beyond.[70]

1. **Malware:** Any malicious software, script, or code developed or used for the purpose of compromising or harming information assets without the owner's informed consent. Malware threats include the following: keyloggers/form grabbers/spyware, sending data to external site/entity, exploitation of backdoors, disabling or interfering with security controls or system/network utilities, initiating brute force or dictionary attacks, RAM scraper, capturing data resident on system, exploitation of command and control channels/servers, downloading/installing additional malware or updates, and redirecting to another site/address.

   SQL injection, cross-site scripting, and unauthorized remote access are attackers' favored methods of stealing data and depositing malware.[71] However, there has been a shift to

[70] This list of threat classes is based on the following industry research and reports: *Threat Landscape, Mid-Year 2013* (ENISA, September 2013), *Internet Security Report – 2013* (Symantec, April 2013), *2013 Data Breach Investigations Report* (Verizon, April 2013), *The Biggest Cybersecurity Threats of 2013* (Forbes, December 2012), *Security Threat Report 2013* (Sophos, December 2012), *2013 Website Security Report* (WhiteHat webinar, April 2013), and *Security Threats to Business, the Digital Lifestyle, and the Cloud* (Trend Micro, December 2012).
[71] Cross-site scripting is a type of computer security vulnerability typically found in Web applications.

malicious Uniform Resource Locators (URL) as the preferred means to distribute malware.[72] An advantage of URLs as a distribution mechanism lies in the fact that URLs are not an easy target for law enforcement takedowns.

With such a high proportion of command and control servers, the U.S. is subject to the highest rate of malware attacks.[73] This is most likely due to a very high concentration of intellectual property and digitized data that resides in the U.S. Anytime attackers who wish to launch a denial-of-service attack can send special commands to their botnets.[74] Command and control servers with instructions to perform an attack on a particular target, and any infected machines communicating with the contacted command and control server will comply by launching a coordinated attack. Additionally, as attackers continue to improve their techniques, they have developed precision-targeted malware that is more dedicated so that it only attacks computers with a specific configuration.

2. **Hacking:** All attempts to intentionally access or harm information assets without authorization or in excess of authorization by thwarting logical security mechanisms. A hacker is an expert computer programmer, or a person who breaks into computers or networks; hackers seek and exploit weaknesses in a computer system or computer network and gain unauthorized access to the data on that system or network.

   Hacking is usually conducted remotely, allowing attackers the benefits of anonymity and scalability; automated tools and basic scripting, often written by someone else and made available to attackers, make many varieties of hacking extremely easy to conduct, and allow for attacks against multitudes of potential victims. Forms of hacking include: exploitation of default or guessable credentials, use of stolen login credentials, brute force and dictionary attacks, exploitation of backdoor or command and control channels, exploitation of insufficient system authentication (e.g., no login required), SQL injection, remote file inclusion, and abuse of functionality. In addition, the exploitation of zero-day vulnerabilities and drive-by Web attacks are on the rise.[75]

---

[72] A URL is an Internet address, identifying the location of a file on the Internet, consisting of the protocol, the computer on which a file is located, and a file's location on a specific computer.
[73] Command and control servers are centralized machines that are able to send commands and receive outputs of machines as part of a botnet.
[74] A botnet is a collection of Internet -connected programs communicating with other similar programs in order to perform tasks.
[75] A zero-day vulnerability is one that was previously unknown in a computer application. A zero-day attack or threat is one that exploits the previously unknown vulnerability, meaning that the attack occurs on "day zero" of awareness of the vulnerability. It also means that developers have had zero days to address and patch the vulnerability. Zero-day exploits (the software and/or strategies that use a security hole to carry out a successful attack) are used or shared by attackers before the developer of the targeted software knows about the vulnerability.

3. **Social Engineering/Social Tactics:** Deception, manipulation, and intimidation, and savvy threat agents know how to use this to their advantage. Social networks, including Facebook and LinkedIn, are about connecting people, and a convincing-looking profile of a company or person followed by a friend or connection request can be enough to get a social engineering scam rolling. These threats include: pretexting (classic social engineering), solicitation/bribery, various phishing techniques (or any type of *ishing), and elicitation (subtle extraction of information through conversation).

4. **Misuse:** Use of entrusted organizational resources or privileges for any purpose or in a manner contrary to that which was intended. These actions can be malicious or non-malicious in nature. They include: embezzlement, skimming, and related fraud, use of unapproved hardware/devices, abuse of system access/privileges, misappropriation of private knowledge, and inappropriate web/Internet usage.

5. **Advanced Persistent Threats/Targeted Attacks:** Threats that are highly sophisticated and carefully constructed. The intention behind the attacks is to gain access to a network and steal information quietly. They take a low-and-slow approach that often makes them difficult to detect, giving them a high likelihood of success.

   An advanced persistent threat is really is a team of skilled hackers that have been given a target and work day and night to penetrate that account. Several of these types of threats are supported by their military (like China and Iran), which is essentially industrial espionage by nation-states, go after both civilian and military targets.

   In first half of 2013, targeted attacks demonstrated their effectiveness in achieving their objectives. The biggest innovation in targeted attacks was the emergence of watering hole attacks, which involve compromising a legitimate website that a targeted individual might visit and using it to install malware on their computer.

   Cyber espionage attacks, in particular, reached a dimension that went far beyond expectations. The proliferation of mobile devices delivers a wide exploitation surface for these kinds of threats. Toolkits exist for creating a variety of malware and for attacking websites. Mobile spyware applications might become strong tools for advanced persistent threats targeting bring-your-own-device environments.

6. **Bring-Your-Own-Device Trend:** Users are increasingly using their devices as they would their personal computers, and by doing so are opening themselves up to web-based attacks the same as they would if they were operating a desktop computer. All this means is that the flood of iPhones, Google Android phones and other devices making their way into the workplace are opening up another potential gateway for attackers that needs to be secured. For attackers, it is likely as well that there will be more attempts to circumvent the

application review and detection mechanisms mobile vendors use to guard their application markets.

7. **Cloud Computing:** With more organizations putting more information in public cloud services, those services become large targets, and can represent a single point of failure for the enterprise. Security must continue to be an important part of the conversation with cloud providers, and the needs of the business should be made clear.

8. **Code Injection:** The exploitation of a computer bug that is caused by processing invalid data. Code injection can be used by an attacker to introduce (or "inject") code into a computer program to change the course of execution. A notable issue with regard to this threat is attacks against popular Content Management Systems.[76] Due to their wide use, popular sites make up a considerable attack surface that has drawn the attention of cyber criminals. Cloud service provider networks are used increasingly to host tools for automated attacks, thus implementing an important step in code injection attack vectors.

9. **HTML 5:** HTML 5's cross-platform support and integration of various technologies opens up new possibilities for attack, such as abusing Web Worker functionality. Even with an increasing amount of attention being paid to HTML 5 security, the newness of it means that developers are bound to make mistakes as they use it, and attackers will look to take advantage. So, there may be a surge in HTML 5 oriented attacks in 2013, then followed by a gradual decline as security improves over time.

10. **Botnets:** Although there is a shift to URLs for malware infection (see malware section), there are developments with regard to this threat. For example, there is increased use of peer-to-peer botnets. Such botnets are difficult to locate and take down. Botnets have high availability and are widely distributed.

    It is easy is to create botnet infrastructures by misusing weaknesses in the security of massively deployed devices. Browser-based botnets are another example on how easy is to create a very large botnet infrastructure. Browser-based attacks still remain the most reported threats, whereas Java remains the most exploited software for the materialization of this threat.[77]

11. **DNS Reflection Attacks:** Also known as DNS amplification attacks, these are a type of distributed denial-of-service attacks that take advantage of the fact that a small DNS query can generate a much larger response. When combined with source address spoofing, an attacker can direct a large volume of network traffic to a target system by initiating

[76] A content management system is a system used to manage the content of a website; it is a computer program that allows publishing, editing, modifying, and maintenance of content from a central interface.
[77] As of August 22, 2013, research shows that Java was the most targeted endpoint technology for cyber attacks.

relatively small DNS queries. Attackers seem to have adopted the DNS reflection technique to launch amplification attacks, an old technique that has made a come-back.

12. **Identity Theft:** This threat led to some of the most successful attacks by abusing Short Message Service (SMS) forwarders to achieve significant financial fraud.[78] These attacks were based on known financial trojans (e.g., Zeus, SpyEye, Citadel) that have been implemented on mobile platforms and attack two-factor authentication. A significant source for applying this threat remains social media. It is worth mentioning that an increase in malicious browser extensions has been registered, aimed at taking over social network accounts.

13. **Search Engine Poisoning:** Exploits the use of search engines (i.e., Google, Yahoo, Bing) to spread malware and viruses. As with many other threats, search engine poisoning has gone mobile; there are some reports of malicious mobile applications performing search engine functions. Search engine optimization poisoning attacks have been identified primarily on popular websites using cross-site scripting or cross-server scripting.

14. **Malvertising:** Malvertising means that legitimate websites can be impacted without being compromised. It opens an avenue of attack that hackers can use to compromise a website without having to directly hack the website itself. Using malicious advertisements, attackers silently infect users, often by installing dynamically created malware that antivirus programs alone are unable to detect.

[78] SMS is a text messaging service component of phone, Web, or mobile communication systems. SMS forward is an application that allows an individual to send a notification of a received or missed call to a specified phone or e-mail.

Appendix C
Sample ROE[79]

Audit of X

Job Code

Date

Agency Logo

Rules of Engagement

Agency Name
Office of Inspector General
City/State/Zip Code

[79] All **bolded** wording in this appendix should appropriately be completed by the representative OIG. References to "agency" apply to any responsible office, component, or governing body. The source of this ROE is DHS OIG.

Table of Contents

1.0 Background and Objective

The **agency**, Office of Inspector General (OIG), has initiated an audit of **the agency's computers/networks/devices**. As part of this audit, we will perform testing to ensure **X** is adequately protected. Security testing is an important element in evaluating information technology (IT) security controls because it helps determine whether those controls have been implemented and are operating as intended.

The overall objective of this security testing is to determine X according to **agency guidelines and requirements**. This Rules of Engagement (ROE) document outlines the specific plans and testing efforts for the evaluation. This ROE contains information on the OIG's information security testing methodology and identifies steps that the OIG and **the agency** will take to minimize the risk of disrupting operations during testing. Specifically:

- The OIG will make every reasonable effort to limit the operational impact of testing.
- **The agency** should make every reasonable effort to facilitate the testing to help ensure the timely completion of the review.
- The OIG and the agency will comply with this ROE to ensure minimal impact on **the agency** operations and business activities.

2.0 Methodology

We will use software tools to perform security controls testing by connecting a testing computer to the **agency** network. The software tools will collect data from selected **agency computers/networks/devices** and the data will be analyzed to determine system vulnerabilities, security patch installation, and configuration settings. Settings for individual software testing tools will be provided to **the agency** upon request.

The agency should note that firewalls, intrusion prevention systems, disabled remote registry services, and host-based security can prevent scans from completing. A testing location will be selected to minimize the impact of these security controls while still providing full access to **the agency's computers/networks/devices** located on the network under review. If adequate network access cannot be resolved from the designated testing location, **the agency** will provide direct access for local testing of **the agency's computers/networks/devices**.

Staff from the OIG will perform all testing. All personnel and technical specialists assigned to the audit hold relevant security clearances. Testing will be performed using software tools. Information on testing tools can be found in Appendix C.

3.0 Scope

The general scope of the testing may include selected **agency computers/networks/devices** that process or contain sensitive information. Domain and root-level administrative access is needed to perform the testing.

4.0 Type of Scans

The OIG will evaluate selected **agency computers/networks/devices** for adherence to **X** requirements. **X** (testing tool) will be used to perform these **X** (type of scans). More information on **the testing tools** to be used can be found in Appendix C.

4.1 Any Additional Type(s) of Scans

The OIG will use **X** (testing tool) to determine **X**. In addition, these scans will be used to identify **X**. More information on **this tool** can be found in Appendix C.

4.2 X Penetration Testing Objective

Upon the discovery of significant or multiple vulnerabilities, the OIG will use **X** (testing tool) to identify and isolate specific exploits that could put systems and data at risk. Testing will be performed on singular **agency computers/networks/devices** only. More information on **this tool** can be found in Appendix C.

5.0 General Rules of Engagement

1. This ROE document is compulsory and will not be departed from without first obtaining written concurrence from the OIG and an authorized representative from the **agency's** Office of the Chief Information Officer (OCIO).

2. Scans may only be postponed or suspended as directed by OIG or **agency's** ROE signatory official. Such termination and justification will be documented in accordance with Appendix B of this ROE. In the event that testing causes a service outage, the **agency** monitor may alert the **agency** Chief Information Security Officer (CISO) or its designated representative to suspend testing.

3. Personnel from **the agency** and other applicable IT or security personnel are encouraged to observe the OIG's testing.

4. **The agency** is responsible for ensuring that system backups have been performed prior to the start of the security testing and that recovery procedures are in place should an inadvertent outage require system restoration.

5. Prior to commencing the scans, **the agency** will appoint an authorized representative to act as "monitor" of the OIG's activities. The monitor will be **the agency's** primary point of contact for the OIG team during the testing. The OIG team will rely on the monitor to answer any questions concerning systems and related IT devices, give final authorization to test any vulnerabilities discovered on **agency computers/networks/devices**, and provide any additional information needed on unanticipated factors affecting the audit that may arise during the testing.

6. The monitor(s) for the testing are:

Name	Phone number(s)	Email address

7. The OIG's testing will be conducted at **the agency** facilities identified in Appendix A.

8. The OIG will conduct testing on the dates and at the times specified and agreed to by the parties. The dates and times will be closely coordinated with **the agency**. The monitor will coordinate and ensure, as appropriate, the involvement of **agency** officials and adherence to applicable **agency** policies and standard operating procedures that could have an impact on the scan activities and the information systems being tested.

9. The OIG will perform testing using OIG-owned laptop computers. Under no circumstances will OIG-owned equipment be relinquished from the control of OIG for any reason. **The agency** may scan the OIG testing laptop for vulnerabilities prior to network connection to verify operating system and software patch status.

10. **The agency** will provide office workspace with AC power and at least one internal network drop at the identified facility. In accordance with the testing methodology, after obtaining a network connection and other information about **the agency's** internal IT environment, the OIG team will begin testing.

11. The OIG will require administrator access to the systems being tested. Administrator access will be provided by (1) **the agency** establishing a separate administrator account for testing (e.g., IGTest), or (2) through the use, under **the agency's** supervision and control, of an existing administrator account. If possible, any separate testing accounts will be established prior to the arrival of the OIG team to the testing site.

12. Under no circumstances will the OIG testers modify any system configuration without prior written consent from **the agency's** OCIO.

13. If the OIG team inadvertently views user files or any other data contained in **the agency's** IT environment that are part of a government agency system of records on individuals, this information will be kept confidential in a manner consistent with the Privacy Act (5 U.S.C. §552a) and any other applicable **agency** regulations.

14. To avoid disruption to **agency** IT operations, in addition to the above precautions, the OIG team will:

    A. Ensure that **agency** or system personnel identify potentially sensitive devices prior to testing.
    B. Keep a journal of comments in text and screen-shots documenting the OIG's activities and times during the testing.
    C. Only disseminate discoveries to the authorized representative(s) of the OIG and **the agency**.

15. During testing, audit logs will be used to monitor the testers' activities.

6.0 Documentation Guidelines

The OIG will provide **the agency** with an exit briefing of the assessment activities.

7.0 Confidentiality and Data Security

All audit evidence collected by the OIG will be held at the OIG facility at **X** (OIG office location). The OIG will not disclose any information related to this testing to any unauthorized parties.

8.0 Dispute Resolution

In the event disagreement(s) should arise between **the agency** and OIG during testing, the following individuals will determine the final resolution:

- OIG – **Name and title**
- **Agency** – **Name and title**

9.0 Approval

Signature: ____ **Name** **Title** **Agency**, OIG	______________________ Date
Signature: ____ **Name** **Title** **Agency**	______________________ Date

Appendix A – Agency Sites Where Testing Will Be Performed

List of sites to be visited for **agency computers/networks/devices** testing:

Site Name	Address	Agency Monitor

Appendix B – Termination of Testing Memorandum

This memorandum will establish an understanding between **the agency** and the OIG to ensure that all parties are in agreement on the conditions that may exist and result in the termination of this security testing effort.

The OIG test team will notify the designated **agency** monitor if a significant event should occur during testing that results in the test team or the client desiring a termination of the testing. The monitor should have the knowledge and understanding of the significant events that would lead **the agency** to direct the OIG to terminate the testing.

The reason for the termination must be documented below. The signatures indicate agreement by all parties on the reason for termination of the testing.

Reason for termination of testing:

____

____

Agency OIG

Signature:

____ __________
Date

Name and Title:

____

Agency Management/CIO

Signature:

____ __________
Date

Name and Title:

____

Appendix C – List of Security Testing Tools Available for the OIG's Use

List testing tools to be used and brief description.[80]

[80] Appendix C of this guide lists the testing tools used within the OIG community and provides brief descriptions of each.

Appendix D
Vulnerability Scanning and Penetration Testing Tools

Below is a list of vulnerability scanning, penetration testing, and system security software tools that are used by the OIG Community.[81] The actual use of the tools will be coordinated with the audit team and site personnel to determine the most appropriate tool for the platform assessed. This list does not represent all of the tools available for use, since such tools and scripts frequently change.

Acunetix
Acunetix Web Vulnerability Scanner automatically checks an organization's web applications for Structured Query Language (SQL) Injection, cross-site scripting, and other web vulnerabilities.

Aircrack-ng
Aircrack-ng is a set of tools for auditing wireless networks. Aircrack-ng is an 802.11 Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access-Pre-shared key-cracking program that can recover keys once enough data packets have been captured. It implements the standard Fluhrer-Mantin-Shamir attack along with some optimizations like KoreK attacks[82], as well as the new PTW attack, thus making the attack much faster than other WEP cracking tools.[83]

AirMagnet
Fluke Networks' AirMagnet delivers a complete solution portfolio to ensure security, performance, and compliance of wireless networks to mitigate any issue that threatens an organization's business. Fluke Networks delivers the most accurate solutions for designing, deploying, and optimizing 802.11 a/b/g/n WLANs for maximized performance, security, and compliance. Expert planning and design tools ensure that the wireless network is built to accommodate the highest capacity of users, meet the needs of demanding wireless applications, and perform optimally in the most challenging environments. The AirMagnet Enterprise system provides complete visibility and control of the entire wireless environment, automatically remediating threats and vulnerabilities, proactively alerting on performance problems, and providing detailed compliance reports for regulatory standards such as those for the Payment Card Industry and the Health Insurance Portability and Accountability Act.

[81] This list of licensed vulnerability scanning, penetration testing, and system security software tools used by the OIG Community was obtained from the CIGIE IT Committee report entitled "Survey of Vulnerability and Penetration Testing Usage within the Office of Inspector General Community," and DHS OIG.
[82] A KoreK WEP attack is a statistical cracking method for the recovery of a WEP Key.
[83] A "PTW" attack decreases the number of initialization vectors needed to decrypt a WEP key.

AppDetective
AppDetective, developed by Application Security, Inc., is a network-based vulnerability assessment scanner that locates and assesses the security strength of major applications such as web servers and databases for vulnerabilities. AppDetective will also recommend steps for mitigation.

AppScan
IBM Security AppScan (formerly IBM Rational AppScan) delivers application vulnerability testing and management across the application life cycle for web and mobile apps, including dynamic application security testing and static application security testing, as well as innovative technologies like glass-box testing and run-time analysis that keep up with the latest threats and drive precise, actionable results. AppScan is intended to test web applications for security vulnerabilities during the development process, when it is least expensive to fix such problems.

Burp Suite
Burp Suite is an integrated platform for attacking web applications. Burp Suite allows an organization to combine manual and automated techniques to enumerate, analyze, scan, attack, and exploit web applications.

Cain & Abel
Cain & Abel is a password recovery utility that allows easy recovery of various kinds of passwords by sniffing the network; cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks; recording voice over IP conversations; decoding scrambled passwords; revealing password boxes; uncovering cached passwords; and analyzing routing protocols.

Cain & Abel is made of two major components: Cain is the front-end application that recovers passwords and the password sniffing part; Abel is a Windows NT service that must be installed (locally or remotely) and has the role of scrambling the traffic inside the network, for additional protection.

The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in the protocol's standards, authentication methods, and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources. However, it also ships some "non-standard" utilities for Microsoft Windows users.

Cisco Configuration Assurance Solution 2.0
This product automatically performs regular, systematic audits of the production IP network configuration to diagnose device misconfigurations, policy violations, inefficiencies, and security gaps. It uses a high-fidelity software model of the network infrastructure, accurately simulating the behavior of routers, switches, and protocols, to enable a broad scope of analyses. These

analyses include network configuration and security baseline and postchange audit and analysis functions that are critical to a successful network configuration and change management strategy.

Cisco Security Auditor

Cisco Security Auditor software enables customers to cost-effectively audit their network infrastructure against corporate security policies and industry best practices.[84] Cisco Security Auditor focuses specifically on the problem of determining whether Cisco network devices have been configured in accordance with defined security policies. The software is built on a scalable and flexible auditing framework that allows auditing on a large number and variety of Cisco network devices and allows users to select from a wide range of pre-defined best practice policies, customize those policies, and audit the network for compliance to those policies.[85]

Cisco Password Scanner

Cisco Scanner is a public domain program that can scan a range of IP addresses to find Cisco routers that have not changed the default password.

CiscoWorks Network Compliance Manager

CiscoWorks Network Compliance Manager tracks and regulates configuration and software changes throughout your multivendor network infrastructure (including routers, switches, firewalls, load balancers, and wireless access points), improves visibility into network changes, and tracks compliance with a broad variety of regulatory, IT, agency governance, and technology best practices.

Core Impact

Core Impact, developed by Core Security Technologies, is a security testing software suite that identifies weaknesses and allows exploitation of an enterprise network through a range of attack vectors, including endpoint systems, networks, email users, and web applications. It allows the user to simulate multi-staged attacks to test both perimeter and internal defenses using privilege escalation and pivoting techniques to identify available routes to valuable systems and data.

Core Impact Pro

Core Impact Pro is a commercial-grade, automated penetration security testing software solution designed to allow organizations of all sizes to conduct comprehensive penetration testing across their infrastructure and applications.

---

[84] Note that this product is currently in "maintenance mode" with no further releases planned.

[85] Cisco Security Auditor server is supported on Microsoft Windows 2000 and 2003 and Sun Solaris 8 and 9. The Cisco Security Auditor client is web browser-based and supported on Windows, using Internet Explorer 6.0 or Netscape Navigator 7.1.

Cryptcat
Cryptcat is a lightweight version of Netcat with integrated transport encryption capabilities.

DirBuster
DirBuster is a multithreaded Java application designed to brute force directories and file names on web/application servers.

Dnsmap
Dnsmap is a passive network mapper and normally known as subdomain brute forcer. Dnsmap turns DNS Mapping on or off. Originally released on 2006, it was used by penetration testers during the information gathering/enumeration phase of infrastructure security assessments. After identifying a target company's IP netblocks, domain names, phone numbers, and the like, the tool enables the discovery of all subdomains associated to a given domain. For example, from google.com, it is possible to discover mail.google.com, earth.google.com, sketchup.google.com, desktop.google.com, and so on. Subdomain brute-forcing is another technique that should be used in the enumeration stage, as it is especially useful when other domain enumeration techniques such as zone transfers do not work.

Enum
E**num** unifies traditional telephony and next-generation IP networks, and provides a critical framework for mapping and processing diverse network addresses. It transforms the telephone number—the most basic and commonly used communications address—into a universal identifier that can be used across many different devices and applications (voice, fax, mobile, E-mail, text messaging, location-based services, and the Internet).

Ettercap
Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly, and many other tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Fierce
Fierce domain scan is a reconnaissance tool. Fierce is a practical extraction and report language script that quickly scans domains (usually in just a few minutes, assuming no network lag) using several tactics. Fierce is not an IP scanner. When IP ranges are nowhere near one another, huge chunks of networks can be missed with an IP scanner. Fierce is meant specifically to locate likely targets both inside and outside an organization's network. Only those targets are listed (unless the -nopattern switch is used). No exploitation is performed (unless you do something intentionally malicious with the
-connect switch).

FirePAC
Athena's FirePAC automates the optimization and clean-up of firewall configurations. Rule dependencies are analyzed, redundant rules are removed, and most used rules are placed in an optimized rule order. Because analysis is performed off-line, no direct connection to an organization's firewall is required and what/if modeling can be undertaken without posing any risk to perimeter or internal security, or network availability. The risks posed by dangerous firewall rules represent a critical vulnerability to an organization's overall security.

Firewalk
Firewalking is a technique that employs trace route-like techniques to analyze IP packet responses to determine gateway access control list filters and map networks. The Firewalk tool employs the technique to determine the filter rules in place on a packet forwarding device.

GFI Languard™
GFI Languard is a network security and vulnerability scanner that gives an organization the capability to perform multi-platform scans (Windows, Mac Operating System, and Linux) across all environments, including virtual machines, to analyze the organization's network security setup and status. GFI Languard scans computers, as well as a number of network devices such as printers, routers, and switches; identifies and categorizes security vulnerabilities; recommends a course of action; and provides tools that can be used to resolve problems. The scanning software integrates with more than 2,500 critical security applications in the following categories: antivirus, anti-spyware, firewall, anti-phishing, backup client, VPN client, patch management, web browser, instant messaging, peer-to-peer, disk encryption, data loss prevention, and device access control. GFI Languard's network auditing capability gives a comprehensive view of an organization's network: what USB devices are connected, what software is installed, any open shares, open ports and weak passwords in use, and hardware information.

John the Ripper
John the Ripper is a fast password cracker, currently available for many distributions of UNIX, Windows, Disk Operating System, BeOS, and OpenVMS. Its primary purpose is to detect weak UNIX passwords. Besides several crypt(3) password hash types most commonly associated with various UNIX systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version.

Kismet
Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card that supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plug-ins that allow sniffing other media. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time,

decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

LANScanner

LANScanner is designed for searching local network for files (i.e., movies, music, documents). While scanning, the program memorizes the network's structure. Using a multithreading technique, searching operations are much faster. Features include IP ranges (inclusion/exclusion), network neighborhood scanning, file/folder download, download resumption after connection break, saving search results as text or Hypertext Markup Language (HTML) file, skipping selected shares (floppy drives), folders exploration, and advanced search options.

LSADump

LSADump is an application that is used to gather Windows password hashes from computers running Windows.

Maltego

Maltego is an open source intelligence and forensics application. Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist within the scope of your infrastructure. The unique perspective that Maltego offers to both network- and resource-based entities is the aggregation of information posted all over the Internet. Whether it is the current configuration of a router poised on the edge of your network or the current whereabouts of your vice-president on his international visits, Maltego can locate, aggregate, and visualize this information.

Metasploit®

A collaboration of the open source community and Rapid7, Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments. The software also helps security and IT professionals prevent data breaches by efficiently conducting broad-scope penetration tests, prioritizing vulnerabilities, and verifying controls and mitigations.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer is a free scanning tool that provides a streamlined method to identify missing security updates and common security misconfigurations within Microsoft Windows, Windows components (i.e., Internet Explorer), and other Microsoft products. To assess the security state of an organization's Windows machines, the Analyzer includes 64-bit installation, security update and vulnerability assessment checks, and support for the latest Windows Update Agent and Microsoft Update technologies. Microsoft Baseline Security Analyzer will not scan or report missing non-security updates, tools, or drivers.

ModemScan
ModemScan is a graphical user interface for Microsoft Windows software, which facilitates the auditing and discovery of modems and fax machines. This type of software is commonly referred to as a wardialer or war dialer.[86]

Nbtdump
Nbtdump lists NetBIOS information from Windows and *NIX Samba servers such as shares, user accounts with comments, and the password policy.

Nbtenum
Nbtenum is a command prompt Win32 information enumeration utility. Using null sessions, Nbtenum can retrieve user lists, machine lists, share lists, name lists, group and member lists, and password and local security authority policy information. This tool is used at the command prompt and the output is an HTML file.

Nessus (Professional Feed)
Tenable Network Security's Nessus performs network vulnerability assessment scans to identify hosts and selected vulnerabilities at operating system and application levels for a pre-defined range of IP addresses. Commercial organizations that use the Tenable Nessus vulnerability scanner must purchase a Professional Feed subscription to scan their network, obtain support, receive updates to their database of vulnerability checks, and perform compliance auditing. Subscribers to the professional feed receive immediate access to:

- The newest Tenable Nessus plug-ins as soon as they are released.
- Perform an unlimited amount of complete Payment Card Industry Data Security Standard compliance audits.
- Perform web application audits of custom and embedded applications to test for cross-site scripting, SQL injection, and more.
- Conduct application, router, and SQL database configuration audits against CERT, CIS, DISA STIGs, Gramm–Leach–Bliley Act, Health Insurance Portability and Accountability Act**,** NIST Security Content Automation Protocol, Federal Desktop Core Configuration, NSA, and Payment Card Industry standards.[87]
- Conduct content audits such as adult content, personally identifiable information (credit cards, Social Security numbers, etc.) in corporate spreadsheets, and more.
- Security Content Automation Protocol vulnerability checks to detect and audit control system devices.

[86] Wardialing (also known as telephone scanning or war dialing) is the practice of dialing all the phone numbers in a range in order to find those that will answer with modem or fax tones.
[87] The Federal Desktop Core Configuration is a list of security settings recommended by NIST for general-purpose computers that are connected directly to the network of a U.S. Government agency. It applies only to Windows XP and Vista desktop and laptop computers.

- Virtual Appliance – access to a download of a Nessus 4 VMware Virtual Appliance, which works with VMware ESX, Server, Workstation, and Fusion.

Netcat
Netcat is a computer networking service for reading from and writing network connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Netcat is designed to be a dependable "back-end" device that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool since it can produce almost any kind of correlation you would need and has a number of built-in capabilities.

NetStumbler
NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of WLANs using the 802.11b, 802.11a, and 802.11g WLAN standards.

Newt
Newt is the Nessus vulnerability assessment scanner for a Windows platform.

NeXpose
NeXpose is a vulnerability scanner used to identify vulnerabilities across all of an organization's IT assets and entire environment by leveraging one of the largest vulnerability databases. It conducts more than 85,000 vulnerability checks for more than 28,000 vulnerabilities across physical and virtual networks, operating systems, databases, and web applications. NeXpose identifies all assets within physical and virtual networks, identifies exploits and malware attacks that can breach vulnerabilities identified in an organization's environment, mimics an attack to find vulnerabilities, and validates whether vulnerabilities are exploitable in an organization's environment. The results of these vulnerability scans are then translated into a Real Risk score to help understand an organization's true risk exposure.

NGS SQuirreL
NGS SQuirreL is a vulnerability assessment tool for relational database management system infrastructures. Not only does it identify the weak points in security stature, but it allows systems professionals and database administrators to assess the level of security vulnerabilities quickly and accurately and fix those vulnerabilities identified. NGS provides several SQuirreL tools, including those on the following platforms: Microsoft SQL Server, Oracle, MySQL, IBM Informix, IBM DataBase2, and Sybase ASE.

Nikto
Nikto is an open source web server scanner that performs comprehensive tests against web servers for multiple items, including more than 6,500 potentially dangerous files/Common Gateway Interfaces, checks for outdated versions of more than 1,250 servers, and version-specific problems on more than 270 servers. It also checks for server configuration items such

as the presence of multiple index files and Hypertext Transfer Protocol (HTTP) server options, and will attempt to identify installed web servers and software. Scan items and plug-ins are frequently updated and can be automatically updated.

Nmap
Nmap is a free and open source utility for network exploration, network inventory, and security auditing. Nmap crafts and transmits network traffic to determine what hosts are available on a network, as well as running services, operating systems, and port information for each host.

N-Stalker
N-Stalker is a web application security scanner used to search for vulnerabilities such as SQL injection, cross-site scripting, and known attacks.

Open Vulnerability Assessment System
The Open Vulnerability Assessment System is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. It is available as free software and maintained on a daily basis. Its dedicated contributors and sponsors include penetration testers, power users, security researchers, and academia.

Oracle 8i Benchmark Tool
A CIS product, the Oracle 8i Benchmark Assessment Tool operates on Windows, Linux, and Sparc Solaris platforms and evaluates Oracle 8i instances against CIS Oracle 8i Benchmark v1.2.0.

Oracle Password Checker (Cracker)
Checkpwd 1.23 is one of the fastest dictionary-based password checkers for Oracle databases. This is a useful tool for database administrators to identify Oracle accounts with weak or default passwords. Version 1.23 contains a version that only shows that a password is weak but not the password itself. Checkpwd reads the password hashes from the view dba_users and compares the hashkeys with the hashkeys calculated from a dictionary file.

Proxychains
Proxychains is a Linux dynamically loadable library that will intercept any TCP and UDP traffic from a specific process and tunnel it over HTTP, SOCKS4, or SOCKS5 proxy.

PSTools
This tool is a set of command line utilities that allow an individual to manage local and remote systems.

PuTTY
PuTTY is a free implementation of Telnet and Secure Shell for Windows and UNIX platforms, along with an xterm terminal emulator. Use of PuTTY, PuTTy Secure Copy Program, PuTTy Secure File Transfer Program, and Plink is illegal in countries where encryption is outlawed.

Pwdump
Pwdump is the most popular password dumping utility for Microsoft Windows 2000/XP/2003/Vista.

RainbowCrack
RainbowCrack is a computer program that generates rainbow tables used for password cracking. It differs from conventional brute force crackers in that it uses large pre-computed tables called rainbow tables to drastically reduce the length of time needed to crack a password. RainbowCrack-Online enables businesses and individuals to assess their password policies by providing access to pre-generated hash tables

Router Auditing Tool (RAT)
RAT is a free command line configuration scanner for Cisco routers, switches, and PIX firewalls. It can log into Cisco devices to pull the configuration file directly or it can be given a configuration file. It generates HTML reports detailing all configuration items that were checked, highlighting the items that failed. RAT gives detailed information regarding each configuration item for which it checks, including instructions to implement a fix.

Sandstorm Phonesweep
Phonesweep telephone scanner is a wardialer software written to identify modems on a phone line. Phonesweep is a robust multi-line scanner that can dial every number in an organization. Through this process, it will:

- Identify computers running remote access software that bypass corporate firewalls.
- Identify authorized or unauthorized modems that accept incoming calls.
- Evaluate password settings by attempting to log in with easily guessable usernames and passwords.

Samba
Samba is a free software re-implementation of the Server Message Block/Common Internet File System networking protocol. Samba provides file and print services for various Microsoft Windows clients and can integrate with a Windows server domain, either as a primary domain controller or as a domain member. It can also be part of an AD domain.

Samba runs on most UNIX and UNIX-like systems, such as Linux, Solaris, AIX, and the BSD variants, including Apple's Mac OS X Server (which was added to the Mac OS X client in version 10.2). Samba is standard on nearly all distributions of Linux and is commonly included as a basic system service on other UNIX-based operating systems as well. Samba is released under the GNU General Public License. The name Samba comes from Server Message Block, the name of the standard protocol used by the Microsoft Windows network file system.

Sam Spade

Sam Spade is a general-purpose Internet utility package, with some extra features to help trace the source of spam and other forms of Internet harassment. Sam Spade features include ping, nslookup, whois, IP block, dig, traceroute finger, SMTP Verify, web browser keep-alive, DNS zone transfer, SMTP relay check, Usenet cancel check, website download, website search, E-mail header analysis, E-mail blacklist, and query abuse address.

Security Content Automation Protocol Compliance Checker

The Security Content Automation Protocol Compliance Checker is a tool used to evaluate Security Content Automation Protocol content.[88]

Sid2User/User2Sid

User2sid and Sid2user are two small utilities for Windows NT that allow the administrator to query the Security Accounts Manager to find out a security identifier value for a given account name and vice versa. User2sid.exe can retrieve a security identifier from the Security Accounts Manager from the local or a remote machine, and then Sid2user.exe can be used to retrieve the names of all the user accounts and more. These utilities do not exploit a bug but call the functions LookupAccountName and LookupAccountSid, respectively. These tools can be called against a remote machine without providing logon credentials except those needed for a null session connection. These tools rely on the ability to create a null session in order to work.

SMB Client

Part of the Samba suite, SMB Client is a client that can "talk" to a LAN Manager server. It offers an interface similar to that of the file transfer protocol program. Operations include things like getting files from the server to the local machine, putting files from the local machine onto the server, and retrieving directory information from the server.

snmpcheck

Snmpcheck is a free open source utility to get information via Simple Network Management Protocols (SNMP). It works fine against Windows, Linux, Cisco, HP-UX, SunOS systems, and any devices with SNMP support. It could be useful for penetration testing or systems monitoring. Snmpcheck has been tested on GNU/Linux, *BSD, Windows systems, and Cygwin.

[88] SNMP is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The NVD is the U.S. Government content repository for the Security Content Automation Protocol. The Security Content Automation Protocol combines a number of open standards that are used to enumerate software flaws and configuration issues related to security.

snmpwalk
Snmpwalk is an SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.

Softerra LDAP Administrator™
Softerra LDAP Administrator™ is a LDAP administration tool designed to work with almost any LDAP server, including AD, Novell Directory Services, and Netscape/iPlanet.[89] It simplifies management of LDAP directories providing advanced directory search facilities, bulk update operations, group membership management facilities, and so on. Customizable directory reports equip administrative personnel with information necessary for effective monitoring and audit. Directory data can be exported and imported in many different formats. LDAP-SQL support allows managing LDAP entries using SQL-like syntax and performing LDAP operations that cannot be executed via standard LDAP means.

Softerra LDAP Browser
Softerra LDAP Browser is a freeware product for browsing LDAP directories. It helps to view and analyze LDAP directory data, as well as to get specific information about directory infrastructure and objects by means of directory reports.

Social Engineering Toolkit
The Social Engineering Toolkit is specifically designed to perform advanced attacks against the human element. This tool has become a standard in a penetration tester's arsenal. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

sqlmap
Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester, and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

sqlping3
Sqlping 3.0 is designed to combine all known means of SQL Server/Microsoft SQL Server Data Engine discovery into a single tool, which can be used to identify network servers that an organization never knew existed so they can be properly secured. Sqlping also does brute force password cracking to identify weak passwords.

[89] LDAP is an application protocol for accessing and maintaining distributed directory information services over an IP network.

tcpdump
Tcpdump, a free software product, is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It works on most UNIX-like operating systems: Linux, Solaris, BSD, Mac OS X, HP-UX, and AIX, among others.

tcptraceroute
Tcptraceroute is a traceroute implementation using TCP packets.[90] The more traditional traceroute sends either a UDP or an Internet Control Message Protocol (ICMP) echo packet with a transistor–transistor logic of one, and increments the transistor–transistor logic until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets are taking to reach the destination. However, with the widespread use of firewalls on the modern Internet, many of the packets that traceroute sends are often filtered, making it impossible to completely trace the path to the destination. However, in many cases, these firewalls will permit inbound TCP packets to specific ports on which hosts sitting behind the firewall are listening for connections. By sending TCP SYNchronize packets for default port 80 instead of UDP or ICMP echo packets, tcptraceroute is able to bypass the most common firewall filters.

THC-Hydra
THC-Hydra is a fast network logon cracker that supports many different services. It is a login hacker for Samba, file transfer protocol, post office protocol 3, Internet message access protocol, Telnet, HTTP Auth, LDAP, network news transfer protocol, MySQL, virtual network computing, ICQ, Socks5, PC Network File System, Cisco, and more. Software includes secure socket layer support and is part of Nessus.

TSEnum
TSEnum, which stands for Terminal Services Enumeration, is a tool for scanning for the presence of Microsoft Windows terminal servers.

TSGrinder
TSGrinder is a free tool that allows an individual to perform brute force password guessing in a terminal server environment. Specifically, it is a dictionary-based attack tool and supports multiple attack windows from a single dictionary file.

VNCcrack
VNCcrack is an offline password cracker for the VNC® challenge/response protocol. If one can somehow observe a virtual network computing authentication, then VNCcrack can run a dictionary attack against the exchange and attempt to find the password. It works by scanning

[90] Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.

a packet capture file (as generated by the common tcpdump tool) for virtual network computing challenge/response exchanges, then checks against a preexisting word list.

w3af
W3af, the Web Application Attack and Audit Framework, is a complete environment for auditing and attacking web applications. This environment provides a solid platform for web vulnerability assessments and penetration tests.

WebInspect
HP's WebInspect performs web application security testing and assessment for complex web applications and web services, built on emerging Web 2.0 technologies. WebInspect identifies security vulnerabilities that are undetectable by traditional scanners.

WebScarab
WebScarab is a framework for analyzing applications that communicate using the HTTP and HTTP Secure protocols. It is written in Java and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plug-ins. In its most common usage, WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser. WebScarab is able to intercept both HTTP and HTTP Secure communication. The operator can also review the conversations (requests and responses) that have passed through WebScarab.

WEPCrack
WEPCrack is an open source tool for breaking 802.11 WEP secret keys.

Wikto
Wikto is a tool that checks for flaws in web servers. It provides much the same functionality as Nikto but adds various interesting pieces of functionality, such as a back-end miner and close Google integration. Wikto is written for the Microsoft .NET environment, and registration is required to download the binary or source code.

Windows GoldDisk
Windows GoldDisk was developed by the military for non-classified systems to assist system administrators in securing systems and applications in accordance with the guidance found in the DISA STIGs, checklists, and applicable CIS benchmarks. It covers Windows 2000 (Pro, Member Server, and Domain Controller), Windows XP, Windows 2003 (member server and Domain Controller), IIS 5, IIS 6, Microsoft Office, Netscape Navigator, Internet Explorer, and several antivirus products.

Wireshark®

Wireshark is a network protocol analyzer for UNIX and Windows. It lets you capture and interactively browse the traffic running on a computer network. It has a rich and powerful feature set and runs on most computing platforms, including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is freely available as open source, and is developed and maintained by a global team of protocol experts. (**Note:** Wireshark used to be known as Ethereal®.)

Yersenia

Yersenia is a network tool designed to take advantage of some weakness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Appendix E
Objectives for Evaluating an Agency's Cybersecurity Program

Overall Objective
The overall objective of this audit is to determine whether an adequate and effective cybersecurity program and partnerships have been established to protect agency information technology (IT) systems and critical infrastructure from cyber vulnerabilities and threats.[91]

Detailed Sub-Objectives

1. Identify the agency's roles and responsibilities for securing its cyber assets and critical infrastructures.

   A. Determine whether an organizational structure has been established to fulfill the agency's assigned roles and responsibilities as they relate to the protection of its cyber assets and critical infrastructure.
      1) Ensure that the agency has clearly documented its cybersecurity mission and program.
      2) Ensure that personnel clearly understand the agency's mission as it relates to protecting its IT systems or critical infrastructure from cyber threats.
      3) Determine whether the agency has the resources (i.e., staff and budget) necessary to carry out its cybersecurity mission.
      4) Evaluate whether the agency structure effectively addresses the identification, analysis, and mitigation of cyber threats.

   B. Interview management officials to identify the roles and responsibilities each office has in implementing the actions and recommendations outlined in *The National Strategy to Secure Cyberspace*, National Infrastructure Protection Plan, and Comprehensive National Cybersecurity Initiative.

   C. Identify agency efforts to comply with actions resulting from the President's Cyberspace Policy Review.

2. Determine whether the agency has implemented an effective strategic cybersecurity program to protect its IT systems and critical infrastructure from cyber threats and attacks.

   A. Determine whether the agency has developed a strategic implementation plan that outlines its roles and responsibilities and establishes specific timeframes and milestones to provide a clear plan of action for achieving its cybersecurity mission and goals.

   B. Ensure that the agency has developed and implemented policies and procedures documenting the actions to be taken to comply with applicable cybersecurity guidance.

[91] References to "agency" apply to any responsible office, component, or governing body.

   C. Evaluate the adequacy of the policies and procedures developed regarding cyber threats and mitigating the risks of an attack.
   D. Evaluate whether the agency has adequate processes to identify, analyze, and prioritize cyber vulnerabilities and threats.
   E. Evaluate whether any identified security incidents have been reported through the United States Computer Emergency Readiness Team.

3. Ensure that the agency has established performance metrics and outcome measures for implementing the processes and procedures needed to protect its IT systems and critical infrastructure from cyber threats and vulnerabilities.

   A. Identify the performance and outcome measures developed to evaluate the processes and procedures needed to protect IT systems and critical infrastructure from cyber threats and vulnerabilities.
   B. Determine whether performance measures are periodically reviewed and updated.
   C. Determine how often the performance measures are updated.
   D. Determine who is responsible for the development and approval of performance measures.

4. Determine whether the agency is efficiently overseeing its strategy to protect its IT systems and critical infrastructure.

5. Identify agency partnerships with other Federal agencies, State and local governments, and cross-sector groups, including private sector and international entities, to determine the effectiveness of coordination and awareness activities undertaken to protect cyberspace.

   A. Identify significant partnerships the agency has developed in protecting cyberspace.
   B. Ensure that the agency has a process for coordinating with other government agencies and the private sector in responding to cyber security incidents.
   C. Ensure that the agency has a plan to warn the public and private sectors adequately and timely about possible and actual cyber attacks.
   D. Evaluate whether the agency has developed an international cybersecurity information sharing policy.
   E. Assess the steps taken to strengthen operational collaboration with the agency's international counterparts to reduce cyber vulnerabilities and improve incident response and information sharing capabilities.
      1) Determine whether the agency is participating in bilateral cybersecurity meetings and forums to improve operational cybersecurity collaboration efforts.
      2) Identify whether the agency has established partnerships with international organizations, including government and private industry.

Appendix F
Objectives for Evaluating Identity Management

Overall Objective
The overall objective of this audit is to determine whether an agency is meeting Homeland Security Presidential Directive 12 (HSPD-12) implementation requirements.[92]

Detailed Sub-Objectives

1. Determine whether the agency implementation plan adequately addresses HSPD-12.

   A. Ensure that the agency's HSPD-12 implementation plan adequately addresses the security and technical interoperability requirements of HSPD-12.
      1) Compare the agency's implementation plan to the Office of Management and Budget (OMB) Memorandum 05-24 implementing instructions.
      2) Ensure that the implementation plan complies with Federal Information Processing Standard 201 requirements.
      3) Ensure that the plan contains sufficient information regarding the security, interoperability, and deployment of an Enterprise Identity Management System (EIMS) in order to address HSPD-12 requirements (if applicable).

   B. Ensure that interim milestones have been developed in order to meet the agency's updated HSPD-12 implementation deadline.
      1) Review agency implementation activities, HSPD-12 Council meeting minutes, and status reports submitted to OMB to ensure that projected milestones are being achieved.
      2) Evaluate planned implementation activities with actual status to evaluate whether the deadline for issuance of Personal Identity Verification (PIV) cards to all employees and contractors will be met.
      3) Ensure that measures have been developed to track implementation progress.

   C. Ensure that the agency's department-wide cost estimate includes all costs related to the HSPD-12 implementation, such as costs related to component rollout, enrollment centers, cards readers, and system upgrades.

2. Determine whether physical and system security controls have been implemented and are effective in protecting the privacy of personal data collected and processed by EIMS (if applicable).

   A. Evaluate the adequacy of the physical security controls over the personally identifiable information (PII) stored at the EIMS contractor facility and enrollment centers.

[92] References to "agency" apply to any responsible office, component, or governing body.

1) Evaluate the physical access procedures.
2) Ensure that visitor sign-in and access logs are being used and stored on at least an annual basis.
3) Ensure that inspections are conducted of offices and other facilities at least monthly, to ensure that proprietary materials are being adequately safeguarded. Obtain and review reports from those inspections.
4) Ensure that the agency HSPD-12 project management office has developed and regularly updates a list of personnel with authorized access to the facilities where EIMS resides and that appropriate authorization credentials are being issued.
   a. Ensure that there is a process to track lost credentials.
   b. Ensure that there are procedures for the return and destruction of credentials for personnel who no longer work at those facilities.

B. Evaluate whether agency requirements for database security controls have been implemented to protect PII from unauthorized access.
   1) Review agency policies and best practice guidelines for database configuration.
   2) Perform manual checks on the EIMS database to ensure that agency policies and best practices for databases have been implemented.
   3) Perform vulnerability testing on the EIMS database to evaluate the effectiveness of controls implemented.
      a. Ensure that critical security patches and updates have been applied.
      b. Perform penetration testing to ensure that critical vulnerabilities discovered cannot be exploited and compromise PII data.

C. Ensure that agency requirements for account management and access control have been implemented to restrict and control access to EIMS and PII.
   1) Review agency policies and best practice guidelines for account management and access control.
   2) Obtain a copy of access request forms for all administrators and a sample of user accounts to identify roles and permissions.
   3) Review the policy for granting and controlling access to the network domain, local servers and workstations, and software application.
   4) Ensure that quarterly firewall testing at the contractor's facility is being performed.
   5) Perform manual checks on the local servers and workstations to ensure that agency policies and best practices for access controls have been implemented.
      a. Evaluate the methods by which PII data is input, exported, viewed, and destroyed to ensure restrictions and control measures are in place.
      b. Ensure that only authorized users can access PII data.
      c. Ensure that only limited access and permissions are granted when PII is accessed locally, from the network, and through the software application.

D. Evaluate whether agency requirements for Virtual Private Network (VPN) connections have been configured to ensure that PII data is protected when remotely accessed.
   1) Review agency policies and best practice guidelines for VPN implementation and management.

2) Perform manual checks on the EIMS VPN concentrator to ensure that agency policies and best practices for VPN management and configuration have been implemented.
   a. Ensure that the system is accessed remotely only via the VPN or other strong authentication mechanism.
   b. Ensure that two-factor authentication and adequate encryption mechanisms are in place to provide secure VPN connections.
   c. Ensure that appropriate access is granted once a connection is established.
3) Perform vulnerability testing on the VPN concentrator to evaluate the effectiveness of controls implemented and to determine whether critical vulnerabilities discovered can be exploited (through penetration testing) that can compromise PII data.

E. Evaluate whether agency requirements for log maintenance and review have been implemented to ensure the integrity of and accountability for PII data.
   1) Review agency policies and best practice guidelines for database logging and log access.
   2) Perform manual checks on system and network settings and logs to ensure that all accesses to the database are being logged as required by agency policies and best practice guidelines.
      a. Ensure that adequate logs are being kept at the database, software application, local, and network levels.
      b. Ensure that logs are reviewed on a regular basis (i.e., monthly).
      c. Ensure that logs are protected from unauthorized modification, access, or destruction.

Appendix G
Objectives for Evaluating Network Management and Security

Overall Objective
The overall objective of this audit is to determine whether the agency has implemented effective controls for protecting its networks.[93]

Detailed Sub-Objectives

1. Evaluate whether the agency or its organizational components have adequate policies and procedures for standard configurations; a patch and vulnerability management process; review of audit trails; performance of periodic network testing; identification (ID) and authentication mechanisms; and deployment of antivirus software. Ensure that policies and procedures address the following:

   A. Standard configurations for network security devices (Intrusion Detection Systems [IDS], firewalls, and encryption devices), network traffic devices (routers, switches), servers and workstations, and antivirus software.
   B. Change control procedures for network changes.
   C. Review and maintenance of audit trails. For example, system and firewall logs are frequently reviewed for any failed and unauthorized logon attempts, suspicious activities, or unauthoroized or unusual activities on the networks. In addition, the policies and procedures should:
      1) Define security violations (i.e., attempted unauthorized access, unsuccessful logon attempts, accesses to sensitive data and resources, privileged access, access modifications made by security personnel).
      2) Describe procedures for responding to security violations.
      3) Specify procedures for determining the seriousness of violations.
      4) Describe procedures for investigating violations.
      5) Define the process for reporting violations to higher levels of management.
      6) Define access trends and deviations from those trends.
      7) Document disciplinary actions for specific types of violations.
      8) Propose the notification of the resource owner of any violation.
      9) Describe procedures for reporting suspected criminal activity to law enforcement officials.
   D. A patch and vulnerability management process to ensure security patches are tested and installed to mitigate security vulnerabilities identified in a timely manner. Specifically, the process should:

[93] References to “agency” apply to any responsible office, component, or governing body.

1) Create and maintain an inventory of hardware and software deployed over the network.
2) Identify newly discovered vulnerabilities and security patches.
3) Prioritize patch application.
4) Create an agency/component/device-specific patch database.
5) Conduct generic testing of patches.
6) Distribute patch and vulnerability information to local administrators.
7) Verify patches installation through network and vulnerability scanning.
8) Provide training to system administrators to identify new patches and vulnerabilities.

E. A routine security-testing program to evaluate the effectiveness of security controls implemented on networks. New devices should be scanned for proper configuration when they are connected to the network, and servers and network devices should be rescanned after a security patch is applied. In addition, routine testing should:
   1) Reduce the likelihood of unauthorized access by identifying possible security vulnerabilities and misconfigurations on networks devices, servers, and workstations.
   2) Include performing network scanning (semi-annually), vulnerability scanning (semi-annually), password analysis (same frequency as password expiration policy), system log review (weekly), file integrity checkers (monthly), virus detection (weekly), war dialing (annually), and penetration testing (annually).

F. Strong ID and authentication mechanisms. For example, strong passwords should be used when accessing agency networks. Password policies should:
   1) Contain a combination of alphabetic, numeric, and special characters, and should not contain any dictionary word or be the same as user ID.
   2) Not be stored in a clear text file.
   3) Be changed at least every 90 days.
   4) Ensure that vendor-supplied passwords are replaced immediately.
   5) Ensure that concurrent logins are not allowed (i.e., one user ID cannot log onto a system or application more than once during the same session) and group accounts are controlled.
   6) Ensure that accounts are configured to lock automatically after three consecutive failed logon attempts.

G. Antivirus software installation on servers and workstations. Antivirus software should be configured to run continuously in the background, and virus signatures should be updated at least weekly/daily.

2. Evaluate whether the processes for network administration (e.g., backup, disaster recovery, and contingency planning; patch and vulnerability management; user account and password administration; network monitoring; and roles and responsibilities) are adequate. Evaluate whether the following processes:

A. Ensure that backup, disaster recovery, and contingency planning are adequate by interviewing the Information Systems Security Manager or network administrators, and determining the following:
    1) A contingency plan has been developed and tested according to the system's overall security categorization. The contingency plan should be included as one of the appendices to the System Security Plan.
    2) Critical files are backed up to a remote location or removable media (e.g., magnetic tapes) periodically and the media stored off-site.
    3) Arrangements are made for alternate data processing and telecommunication facilities.
    4) Event logs are generated when backup operation is performed.
    5) Fire extinguishers, smoke detectors, sprinkler systems, and emergency exit signs are installed at the network operation center or security operation center visited.
    6) Uninterrupted power supply or electric generators are available to provide backup power in the event of emergency.
B. Ensure that a patch and vulnerability management group is established to create a systematic and accountable process for identifying and applying security patches. The process should include:
    1) Creating and maintaining an inventory of existing hardware and software.
    2) Identifying newly discovered vulnerabilities and security patches.
    3) Prioritizing security patch application.
    4) Creating an agency-specific security patch database.
    5) Conducting generic testing of security patches.
    6) Distributing security patch and vulnerability information to local administrators.
    7) Verifying patch installation through network and host vulnerability scanning.
    8) Training system administrators in using the vulnerability database.
C. Ensure that user account and password administration includes management processes that focus on ID, authentication, and access authorizations, and password administration. Determine whether a well-defined process has been implemented by ensuring the following:
    1) Program official (system owner) maintains a list of authorized users, reviews access authorization listings, and determines whether users' access remains appropriate.
    2) Access authorizations are documented on standard forms and maintained on file.
    3) Security managers review and approve access authorizations and are notified immediately when users are terminated or transferred.
    4) Users sign an "acknowledgment statement" when they are given access. The acknowledgment statement details acceptable rules of behavior as well as consequences of non-compliance.
    5) User access permissions are reviewed at least annually.
    6) Inactive accounts are disabled.
    7) Default passwords supplied by the vendors are changed.
    8) Passwords cannot be viewed in clear text when entered.

D. Ensure that network traffic is monitored continuously and a follow-up process exists for service disruptions, suspicious activities, and ongoing attacks against the network or interconnected systems.
E. Ensure that the roles and responsibilities for administrators are documented in their job descriptions, which should match the administrators' duties. In addition, detailed written instructions should exist and be followed to guide the administrator in perfoming his/her duties.
F. Ensure that all access paths to the networks are identified in the current network topology. The access path diagram should be reviewed and updated whenever changes are made to the network.

3. Evaluate whether security controls implemented on network security devices (firewalls, IDSs, and encryption devices) are effective.

   A. Firewalls
      1) Identify and examine the type of firewalls deployed (packet filters, circuit-level gateways, application-level gateway, and stateful multilayer inspection).
      2) Ensure that firewall devices are secured behind locked doors.
      3) Ensure that firewall logging capabilities are enabled and reviewed frequently.
      4) Ensure that a firewall policy has been developed and defines how the firewall should handle applications traffic such as web, email, or telnet. The policy should describe how the firewall is to be managed and updated. The default firewall policy for handling inbound traffic should be configured to block all packets and connections unless the traffic type and connections have been specifically permitted. In addition, the firewall rule set should always block the following types of traffic:
         a. Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself. (**Note:** This type of packet normally represents some type of probe or attack against the firewall.)
         b. Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. (**Note:** This type of packet likely represents some type of spoofing attempt.)
         c. Inbound traffic containing Internet Control Message Protocol (ICMP) traffic. (**Note:** Since ICMP can be used to map the networks behind certain types of firewalls, ICMP should not be passed in from the Internet, or from any untrusted external network.)
         d. Inbound or outbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. (**Note:** RFC 1918 describes a set of network ranges set aside for so-called "private" use.)
         e. Inbound traffic from a non-authenticated source system containing Simple Network Management Protocol (SNMP) traffic. (**Note:** These packets can be an indicator that an intruder is probing a network, but there are few reasons an

organization or agency might want to allow inbound SNMP traffic, and it should be blocked in the vast majority of circumstances.)

f. Inbound traffic containing Internet Protocol (IP) source routing information.
g. Inbound or outbound network traffic containing a source or destination address of the local host. (**Note:** Such traffic is usually some type of attack against the firewall system itself.)
h. Inbound or outbound network traffic containing a source or destination address of inbound or outbound traffic containing directed broadcast addresses.
i. Ensure that access to the firewall operating system console and any graphic management interface is restricted to authorized users only. The use of encryption and/or strong user authentication and restricting access by IP address can limit access to firewalls.
j. Perform scans with automated tools to evaluate the following:
    1. Firewall internal operating system, firewall engine, and firmware are up-to-date.
    2. Firewall configuration.
    3. Firewall notification, reporting, and analysis capabilities are present.
    4. Packets are captured or logged by the firewalls.
    5. All unused networking protocols are not on the firewall operating system build (if identified, should be removed).
    6. All unused network services or applications are removed or disabled.
    7. All unused user or system accounts are removed or disabled.
    8. All unused physical network interfaces are disabled or removed from the server chassis.

B. IDSs
1) Ensure that incident response procedures are developed for security and intrusion incidents detected.
2) Ensure that IDS rules and signatures are updated frequently.
3) Ensure that access list is maintained for users with administrator access.
4) Ensure that the IDS is configured for the following:
    a. Differentiate between normal and abnormal network traffic patterns and suspicious user activities.
    b. Identify suspicious files and data modified.
    c. Monitor user accounts, system files, and log files for tampering.
    d. Send alerts (by page, E-mail, or other means) when high-level intrusions occur and to minimize alerting resulting from false positives and low-level attacks.
    e. A report module exists to aggregate attacks over a period of time (i.e., hourly, weekly, monthly).

C. Encryption devices
1) Determine the type of encryption devices deployed. (**Note:** Internal network traffic is usually not encrypted. If network traffic is transmitted between corporate offices

that are physically separate, whether down the street, to another state, or to another country, all traffic must be encrypted.)

2) Ensure that the encryption capability is enabled.
3) Ensure that the encryption standard (e.g., Triple Data Encryption Algorithm, Advanced Encryption Standard) complies with Common Criteria Evaluation Assurance Level 4 and/or Federal Information Processing Standard 140-2 accreditation.
4) Ensure that adequate physical security is provided to protect encryption devices from unauthorized access and tampering.
5) Ensure that the management capabilities are secure by using strong encryption, digital certificates, and Digital Signature Standard for strong authentication. Management capabilites may also include proprietary interfaces that are SNMP based, or they could be physical like RS-232 terminal interface. This also includes examination of audit logs, alarm condition detection, and secure download of software updates.
6) Verify that the encryption device only routes traffic from approved networks. The traffic from the encryption device should be sent to a single IP address—the IP address of the target network—or there may be a pool of encryption devices.

4. Evaluate whether security controls implemented on network traffic devices (routers and switches) are effective.

   A. Routers

   Ensure the following by reviewing configuration settings, interviewing administrators, and performing scans with automated scanning tools:

   1) Router Internet Operating System is up-to-date.
   2) Router configuration is maintained off-line and backed up, and access to the router is restricted.
   3) Router configuration is well documented and commented.
   4) Router users and passwords are configured and maintained.
   5) Password encryption is in use; enable secret is in use.
   6) Enable secret is difficult to guess and knowledge of it is strictly limited (if not, change enable secret immediately).
   7) Access restrictions are imposed on Console, Auxiliary, and Virtual Terminal Lines (VTL).
   8) Unneeded network servers and facilities are disabled.
   9) Necessary network services are configured correctly (e.g., Domain Name System).
   10) Unused interfaces and VTLs are shut down or disabled.
   11) Risky interface services are disabled.
   12) Port and protocol needs of the network are properly identified and checked.
   13) Access lists to restrict traffic to identified ports and protocols. In addition, access lists should block reserved and inappropriate IP addresses.

14) Static routes are configured where necessary.
15) Routing protocols are configured to use integrity mechanisms.
16) Router's time of day is set accurately, maintained with Network Time Protocol (NTP).
17) Enable logging capability with time stamp and log recipient hosts are identified and configured.
18) Logs are reviewed and archived in accordance with security policy.
19) SNMP protocol is disabled or enabled with good community strings and Access Control Lists (ACL).

B. Switches

Ensure the following by reviewing configuration settings, interviewing administrators, and performing scans with automated scanning tools:

1) Physical access to switches is restricted to authorize personnel only.
2) Latest stable version of the Internetwork Operating System is installed on each switch.
3) An enable secret password is created.
4) Switches are managed out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate virtual local area network (VLAN) number for in-band management.
5) Switches are configured with session timeouts and access privileges.
6) A warning banner is displayed to notify users that "unauthorized access is prohibited."
7) Unnecessary network services (e.g., Transmission Control Protocol small servers, Hypertext Transfer Protocol) are disabled.
8) Only necessary network services are enabled on switches and these services are properly configured.
9) Secure Shell (SSH) with a strong password is used, instead of using telnet to switches.
10) If SNMP is necessary, a strong community string is set for SNMP.
11) Port security is implemented to limit access based on Media Access Control (MAC) address. Auto-trunking on ports is disabled.
12) The switch's port mirroring capability for IDS access is enabled.
13) Unused switch ports are disabled, and are assigned a VLAN number when not in use.
14) Trunk ports are assigned a native VLAN number that is not in use by any other port.
15) The VLANs that can be transported over a trunk are limited to those that are necessary.
16) Static VLAN configuration is used.
17) If possible, disable VLAN Trunking Protocol (VTP). Otherwise, set the following for VTP: management domain, password, and pruning; then set VTP into transparent mode.
18) ACLs are established when appropriate.
19) Logging capability is enabled and event logs are sent to a dedicated, secure log host.

20) Logging is configured to include accurate time information, using NTP and timestamps.
21) Logs are reviewed for possible incidents and archived in accordance with the security policy.
22) Authentication, authorization, and accounting features are used for local and remote access to switch.
23) Switch configuration files are maintained off-line, and their access is restricted to authorized administrators. The configuration file should contain descriptive comments for the different settings to provide perspective.

5. Evaluate whether security controls implemented on servers and workstations are effective. Ensure the following by reviewing configuration settings, interviewing administrators, and performing scans with automated scanning tools:

   A. Unnecessary ports and services are disabled.
   B. Latest security patches are installed to mitigate vulnerabilities.
   C. Servers and workstations are properly configured.
   D. Security backdoors are created on servers and workstations to guard against unauthorized or rogue peripherals (modems, wireless access points), and programs are installed.
   E. Strong passwords are used.

6. Evaluate whether adequate physical security controls have been established to restrict access to network resources. Specifically, evaluate whether physical access to network security devices, network traffic devices, servers, and workstations is restricted to authorized users. Access should be limited to personnel with a legitimate need for access to perform their duties. Management should regularly review the list of personnel authorized to have physical access to its sensitive facilities. Physical security controls may include:

   A. Manual door or cipher key locks.
   B. Magnetic door locks that require the use of electronic keycards.
   C. Biometrics authentication.
   D. Security guards.
   E. Photo IDs.
   F. Entry logs.
   G. Logs and authorization for removal and return of tapes and other storage media to the library.
   H. Electronic and visual surveillance systems.
   I. Perimeter fences around sensitive buildings.
   J. Perimeter intrusion alarms.
   K. Computer terminal locks.

Appendix H
Objectives for Evaluating Laptop Security

Overall Objective
The overall objective of this audit is to determine whether the agency has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to government-issued laptop computers.[94]

Detailed Sub-Objectives

1. Evaluate whether the agency has established adequate policies and procedures for inventory management and physical security of government-issued laptops.

   A. Ensure that the agency has established adequate and effective procedures for inventory management.
      1) Assess whether the agency has established a process to ensure that newly acquired laptop computers are immediately entered into a property management system.
      2) Verify that the inventory includes all of the following required items:
         a. Serial and/or seat number of laptop. (**Note:** A seat is a node on a network that can communicate using interprocess communication services. A seat is where entities and ports reside.)
         b. Name of owner or user of laptop.
         c. Purpose or use of laptop.
         d. Location of laptop.
         e. Laptop asset tag number.
      3) Ensure that the laptop computer inventory includes information on the software (including version number) of each laptop or group of laptops.
      4) Evaluate the accuracy of inventory records by verifying that correct information is on file for the subset of laptops included in the manual checks. Include a list of any identified inaccuracies.
      5) Assess whether employee and contractor exit procedures include the return of laptops to the local property administrator.
      6) Ensure that the agency has policies and procedures regarding corrective or disciplinary actions resulting from lost or stolen laptops.
      7) Assess whether the agency is aware of any lost or stolen laptops. If so:
         a. Ensure that the incident was reported and investigated.
         b. Identify whether appropriate corrective actions were taken regarding the responsible employee(s) (e.g., disciplinary action, remedial training).

[94] References to "agency" apply to any responsible office, component, or governing body.

8) Evaluate whether the agency has established adequate procedures for maintaining inventory records, conducting inventory reviews, and employee exit processing.

B. Ensure that the agency has established adequate and effective procedures for appropriately disposing of unneeded laptops.
   1) Verify that excess laptops are secured while awaiting preparation for disposal.
   2) Analyze whether the agency has a process for ensuring that the hard drives and memory (e.g., random access memory [RAM], synchronous dynamic random access memory [SDRAM]) of laptops scheduled for reuse have been cleared, including the use of an acceptable clearing process.
      (**Note:** Clearing a hard drive requires overwriting all locations with a pseudo-random pattern twice, overwriting all locations with a known pattern, and then verifying the procedure by randomly re-reading [a minimum of 1 percent recommended] the overwritten information.)
   3) Identify whether the agency has a process for sanitizing hard drives and memory (e.g., RAM, SDRAM) of laptops scheduled for disposition (including return to manufacturer for repair or return to vendor upon completion of lease).
   4) Assess that the agency uses an acceptable sanitizing process.
      (**Note:** Sanitizing a hard drive requires incineration or degaussing [see approved degausser list at http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-9-12.pdf].)
   5) Ensure that the agency removes all labels or markings prior to disposal.
   6) Verify that the agency properly disposes of its drives through incineration in an Environmental Protection Agency-approved facility, burial in a landfill, or recycling.
   7) Ensure that the agency maintains records of the clearing, sanitization, and disposition of laptop computers.
   8) Verify that degaussing equipment (automatic degausser or degaussing wand), where used, is periodically tested to verify that the equipment is functioning properly.
   9) If available, judgmentally select a sample of cleared and/or sanitized laptops to verify that data cannot be accessed. Alternatively, review available documentation to verify that disposed laptops were properly cleared and/or sanitized.

C. Ensure that the agency has developed sufficient physical security safeguards.
   1) Conduct a tour of the facility to determine, through observation, whether assigned laptops are secured when unattended via a locking cable, locked office, or locked cabinet or desk.
   2) Assess whether unused laptops are stored in a secure location with adequate access controls to prevent unauthorized access, disclosure, damage, modification, or destruction when the laptops are not in use.
   3) For the subset of laptops included in the manual checks, determine whether asset tags have been attached to each laptop computer.
   4) For the subset of laptops included in the manual checks, determine whether the laptops are marked with the highest level of classification of information that has ever been processed or stored on the device.

5) Ensure that employees obtain written approval from the office director before taking a laptop overseas.
6) Identify any anti-theft measures that may serve as best practices, such as travel hard drives and tracking hardware.

2. Evaluate whether adequate logical access controls and wireless security measures are adequate for sensitive data contained on government-issued laptops.

A. Establish and use adequate model systems to ensure that laptops are appropriately configured prior to issuance, and that software is updated as necessary.
1) Ensure that a model system or standard build is used for laptop software installation.
2) If a model system is used, ensure that it addresses:
a. Hardware type and/or model.
b. Operating system version and patch level.
c. Major installed applications (version and patch level).
d. Standard configuration settings.
3) If a model system is used, ensure that the model system or laptop configuration is based on agency, National Institute of Standards and Technology (NIST), or other guidelines. Specify which guidelines are used.
4) Ensure that a personal firewall product is installed on devices with wireless capabilities or that access the network remotely.
5) If a personal firewall is installed, ensure that it is periodically updated and reviewed.
6) Identify whether antivirus software is installed. If yes, determine whether the:
a. Product is periodically updated.
b. Software employs resident (as opposed to on-demand) scanning, to include boot-up and installation of new software.
(**Note:** A resident virus scanner runs constantly, and automatically checks files for viruses as they are opened. An on-demand scanner requires a specific action to begin scanning.)
b. The laptop used to connect to the agency's network remotely has Virtual Private Network (VPN) software installed. If VPN software is installed, ensure that it complies with Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.
7) Test a subset of laptops to ensure that they are configured to lock automatically after 5 minutes of inactivity.
8) Conduct scans, such as Internet Security Systems Internet Scanner scans and Superscan Scans.
9) For any deviations from agency configuration baseline guides, determine if an exception or waiver has been submitted and approved by the agency.

B. Evaluate whether appropriate encryption measures have been implemented to protect sensitive data on the laptop computers.

1) Identify whether encryption has been implemented on all laptops. If yes, ensure that the encryption used Advanced Encryption Standard and FIPS 140-2, Security Requirements for Cryptographic Modules.
2) For agencies using approved wireless technologies, ensure that strong data and transmission encryption have been implemented.
   a. Assess whether an Encryption Key Management Plan consistent with agency public-key infrastructure policy authority requirements has been implemented and enforced.
   b. Review whether the Encryption Key Management Plan has been reassessed annually.

C. Ensure that inappropriate files and programs are not stored or installed on laptop computers.
   1) Review whether access to each laptop's system software and hardware is limited to authorized personnel (i.e., ensure that the user does not have administrative or unnecessary privileges on the laptop).
   2) Identify whether the agency conducted reviews, at least semi-annually, of all equipment and software in its offices to ensure that only government-licensed software and equipment are being used, or that appropriate exceptions have been documented. Provide the date of the last official review.
   3) Ensure that inventory reviews are conducted. Determine the adequacy of the review process by comparing the results of the last review with any findings identified during testing.
   4) Assess whether laptops not authorized for classified processing have an external label affixed stating that "This machine is not authorized for classified processing."
   5) Verify that passwords are not stored on or with the laptop, such as cached domain logon credentials.
   6) Examine a sample of laptops to determine whether any suspicious or unusual programs or files are present.

3. Ensure that any built-in wireless, Bluetooth, or infrared devices are disabled or appropriately controlled.

   A. Assess whether the agency received approval for the use of wireless technologies.
   B. Identify whether quarterly security assessments are conducted on approved wireless systems.
   C. Verify that risk mitigation and security plans have been developed to address wireless security vulnerabilities on approved wireless systems.
   D. Evaluate whether appropriate countermeasures been implemented to strengthen the security of wireless laptops, including antivirus software and installation of relevant security patches.
   E. Review whether the following built-in wireless technologies have been disabled if not specifically approved. Check for the presence of each of the following: Windows Device

Manager, Communications Devices, Human Interface Devices, Network Adapters, and Universal Serial Bus Controllers.

Appendix I
Objectives for Evaluating Wireless Security

Overall Objective
The overall objective of this audit is to determine whether the agency has implemented effective controls to ensure that sensitive information processed by its wireless networks and devices are protected from potential exploits.[95]

Detailed Sub-Objectives

1. Evaluate whether the agency has implemented adequate policies and procedures to mitigate the inherent risks associated with the use of wireless networks and devices.

   A. Assess whether the agency has developed requirements, policies, and procedures for its wireless network and devices to adequately address inherent security risks.
   B. Verify whether the agency is in compliance with agency and National Institute of Standards and Technology (NIST) wireless security policies and procedures.
      1) Obtain copies of the agency and NIST wireless security policies and procedures.
      2) Identify the information security standards and requirements for wireless networks and devices.
      3) Assess whether the agency's wireless security policies and procedures are in compliance with applicable agency and NIST guidance.
   C. Ensure that the agency addresses known, reported security risks and vulnerabilities from previous Office of Inspector General (OIG) and Government Accountability Office GAO) audit reports.
      1) Obtain specific GAO and OIG reports related to wireless security at the agency.
      2) Identify any common vulnerabilities or threats that were reported.
      3) If applicable, evaluate whether the agency has addressed and closed the recommendations.

2. Evaluate whether the agency has implemented an effective process to account for its wireless networks and devices and the physical protection of these networks and devices from unauthorized access.

   A. Assess the agency's process for issuing and deactivating wireless devices.
      1) Determine who is responsible for maintaining the agency's inventory and ensuring that it is accurate.
      2) Obtain the agency's policies and procedures for issuing and deactivating its wireless and handheld devices.

[95] References to "agency" apply to any responsible office, component, or governing body.

B. Review the agency's inventories for its laptops, Blackberries, and Bluetooth devices and determine whether the agency can account for the devices issued and assigned to authorized users (Federal and contractor personnel).
   1) Obtain lists of system inventories and users from the agency property office or program management officials.
   2) Obtain inventory review schedules or logs, including when and how often the inventory is updated.
   3) Review and compare a random sample of system inventories with devices held and stored by agency users.
   4) Evaluate whether devices are issued/returned based on user employment status.
   5) Compare equipment issued/received with list of active/departed users and identify whether all equipment issued can be accounted for.
C. Analyze whether the physical security controls over the facilities where the agency's wireless network servers, laptops, and devices are housed are adequate.
   1) Perform on-site physical security assessments of the agency facilities that house its wireless network equipment, access points, and devices, including server rooms and storage closets, to evaluate whether the agency has provided adequate physical security controls.
   2) Evaluate whether the agency is in compliance with agency policies and best practices for the protection of its network equipment, access points, and devices.
   3) Ensure that visitor sign-in and access logs are being utilized and maintained, to track access to system equipment and devices, where appropriate.
   4) Ensure that inspections are conducted of offices and other facilities, at least quarterly, to safeguard physical access to the systems. Obtain and review reports from those inspections.

3. Evaluate whether system security controls have been effectively implemented and properly configured on the agency wireless network and selected devices.

   A. Ensure that agency requirements for account management and access control have been implemented to restrict access to the agency's wireless networks and devices.
      1) Review agency policies and best practices for account management and access control.
      2) Obtain a list of network and BlackBerry server administrators.
      3) Ensure that only authorized users have administrator access to wireless networks and devices.
      4) Sample user accounts to identify roles and permissions.
      5) Evaluate the effectiveness of account management, access control settings, and separation of duties.
   B. Perform wireless scans on selected wireless network equipment and devices, as well as Bluetooth capabilities, to determine whether adequate controls have been implemented.

1) Assess whether system settings and configurations on applicable servers are in accordance with agency and NIST wireless and Bluetooth security policies.
2) Analyze network connections and the agency's wireless security architecture to evaluate the effectiveness of system security controls.
3) Ensure that agency and NIST encryption requirements are implemented on the agency's wireless networks and devices.
4) Assess whether Media Access Control configurations are enabled in accordance with applicable agency and NIST policies.
5) Ensure that Service Set Identification broadcasting configurations are in accordance with agency and NIST policies.
6) Scan to detect any signal leakage from the wireless network or devices.
7) Scan to identify whether any rogue networks or access points are detected.

C. Identify the status of patches deployed on selected agency network equipment, including laptops.
1) Obtain and review agency policies and procedures for patch management of information systems, specifically wireless networks and devices.
2) Identify who is responsible for implementing patches on selected agency wireless network servers and devices.
3) Obtain patch logs and schedules.
4) Examine when and how often the agency implements patches on its wireless network equipment or devices.
5) Perform system security vulnerability assessments on the agency's wireless network servers, including BlackBerry servers and laptops.
6) Ensure that critical security patches and updates have been applied.

D. Review configuration and access control settings for laptops, BlackBerry, and Bluetooth devices to ensure compliance with applicable guidance.
1) Obtain configuration and access control settings for laptops from domain controllers or through manual checks.
2) Utilize software tools, such as BlueAuditor, to obtain configuration settings for BlackBerry and Bluetooth devices.
3) Compare settings on BlackBerry and Bluetooth devices with security configuration checklists.
4) Evaluate whether the agency's laptops, BlackBerry, and Bluetooth devices comply with applicable agency and NIST policies.

4. Evaluate whether the agency actively monitors its wireless networks and devices to enforce wireless security policy.

A. Review and evaluate applicable agency and NIST policies regarding wireless system monitoring and scanning requirements.
1) Obtain applicable agency and NIST policies regarding system monitoring and scanning requirements for its wireless networks and devices.

2) Identify the requirements for system wireless monitoring or scanning.
3) Evaluate whether the agency is in compliance with applicable monitoring requirements.

B. Assess whether the agency performs site surveys to minimize the risks of eavesdropping and signal leakage and identify whether rogue devices are connected to its wireless network.
   1) Identify who is responsible for performing site visits and security assessments on the agency's wireless network or devices.
   2) Interview agency personnel to verify whether the agency performs security assessments on its wireless network as part of site visits.
   3) Obtain site visit logs or schedules.
   4) Obtain site security assessments, reports, and security test logs to verify monitoring activities.
   5) Document what was determined, including any reports of eavesdropping or signal leakage, and what actions, if needed, were or are being taken to address issues identified.

C. Ensure that boundary protection devices such as firewalls and intrusion detection systems (IDS) have been implemented and are working properly.
   1) Obtain an inventory of boundary protection devices, including firewalls and IDSs.
   2) Obtain and review configuration settings.
   3) Ensure that firewall or IDS testing has occurred on selected wireless networks.
   4) Obtain and review firewall and IDS logs to ensure that systems are working properly.

D. Assess whether vulnerabilities identified through testing are being addressed.
   1) If applicable, obtain a list of known vulnerabilities resulting from the agency's security scans or tests.
   2) Identify remediation steps or plans of action to ensure that known weaknesses and vulnerabilities are being addressed.
   3) Ensure that weaknesses identified are being documented and steps are being taken to address known security vulnerabilities.
   4) Analyze whether the actions being taken to address weaknesses are adequate.

Appendix J
Objectives for Evaluating Database Security

Overall Objective
The overall objective of this audit is to determine whether the agency provides adequate system security, integrity, and control over its databases.[96]

Detailed Sub-Objectives

1. Determine whether the databases are protected from unauthorized modification, loss, or disclosure by evaluating the controls that establish and update access to databases.

   A. Ensure that the classification of computing resources has been identified and is consistent with Federal guidelines.
      1) Ensure that written policies and procedures are established, implemented, and approved regarding the classification (criticality and/or sensitivity) of resources, including databases.
      2) Verify that current risk assessments have been performed for database operations.
      3) Ensure that systems processing data have been certified and accredited to provide for security safeguards over sensitive data.

   B. Ensure that the agency has established logical access rules and has consistently assigned and implemented these rules in accordance with Office of Management and Budget A-130 requirements.
      1) Determine whether security policies and procedures have been established. Ensure that these policies and procedures address access controls (to include emergency and temporary access).
      2) Ensure that the Information Systems Security Manager for the agency is identified.
      3) Determine whether the agency maintains a current list of users and their authorized level of access.
      4) Determine whether policies and procedures exist regarding the administration of user identifications and passwords. Identify who is responsible for determining and assigning user access levels.
      5) Ensure that user access rules are defined and reviewed periodically to determine whether they are still appropriate and updated as necessary (i.e., when privileges change).
      6) Ensure that a formal process for transmitting system authorizations, including the use of standardized access request forms that are retained, has been established to reduce the risk of mishandling, alterations, and misunderstandings. Ensure that management approval granting access is documented.

[96] References to "agency" apply to any responsible office, component, or governing body.

7) Determine whether access is authorized and denied according to the established procedure. Ensure that access was:
   a. Authorized for a sample of users.
   b. Removed for terminated employees.
   c. Authorized and removed for users having emergency access.
   d. Authorized and removed for contractors with short-term access.
8) Review the password settings at the application level. Ensure that applications enforce the following:
   a. Passwords must be changed every 30 to 90 days.
   b. Passwords must be at least six alphanumeric characters.
   c. Passwords are prohibited from being reused for at least 180 days (six generations).
   d. Three failed logon attempts lock the user identification (ID).
9) Review the list of application user accounts to ensure that generic user IDs are not being used. Determine whether application users share IDs and passwords.
10) Obtain a list of all application responsibilities. Determine whether users are appropriately assigned to responsibilities based on their job function and access needed.

2. Determine whether audit trails for protecting the database are effective. Examine management's actions to establish, maintain, and evaluate the audit trail reports at the operating system, application, and database levels. The completeness and value of the audit trails will be only as good as the entity's ability to identify the critical processes and related information they may need to deter and detect unauthorized access. (**Note:** This objective should address audits trails over the operating system level as a whole, and the application and database level for selected systems.)

   A. Ensure that the audit trails are properly established.
      1) Verify that security and database activity logs are being generated.
      2) Ensure that written policies and procedures are established, implemented, and approved by management regarding the generation and examination of security and database activity logs. Determine whether the policies and procedures are periodically evaluated to ensure their appropriateness and effectiveness.
      3) Ensure that the procedures for responding to security violations include:
         a. Defining and documenting offenses (i.e., attempted unauthorized access, unsuccessful logon attempts, access to sensitive data and resources, privileged access, access modifications made by security personnel).
         b. Determining the seriousness of violations.
         c. Defining access trends and deviations from those trends.
         d. Reporting violations to higher levels of management.
         e. Investigating violations.
         f. Imposing disciplinary action for specific types of violations.

g. Notifying the resource owner of the violation.
h. Reporting suspected criminal activity to law enforcement officials.

B. Ensure that access controls over audit trail records are established and limited to system administrators and security administrators. Ascertain whether an employee independent of security and database administration reviews the log for security violations.
   1) Identify whether audit logs record who accessed what database as well as the individual rows or columns of a table that were read, changed, or deleted, in addition to recording the execution of the database program. Determine whether Oracle auditing is turned on.
   2) Verify that logs are reviewed daily and whether procedures have been established requiring this review.

C. Ensure that audit trails are properly maintained and evaluated.
   1) Verify whether responsibility has been assigned for receiving notification that audit logs are near capacity.
   2) Determine whether write-once devices are utilized to protect the integrity of the audit trail data against modification.
   3) Verify that only authorized modifications are being made to the security database by administrators.
   4) Review audit logs to ensure that actual or attempted unauthorized, unusual, or sensitive access is monitored. Ensure that security violations are being summarized and reported to senior management.

3. Determine whether the operating system access control program and the database application control program limit and monitor access to law enforcement databases by controlling access to computer hardware and securing database applications supported by the system.

   A. Ensure that operating system controls provide a secure environment in which to run law enforcement database applications.
      1) Determine that passwords are protected. Ensure that access control software enforces the following:
         a. Passwords must be changed every 30 to 90 days.
         b. Passwords must be at least six alphanumeric characters.
         c. Passwords a prohibited from being reused for at least 180 days (six generations).
         d. Three failed logon attempts lock the user identification.
         e. User IDs and passwords are unique to specific individual users and not to groups.
         f. Security administrators are using password analyzers to determine whether password conventions are being followed.
         g. Password files are encrypted.
         h. Security administrators identify inactive IDs and passwords and have implemented a procedure for deletion of inactive IDs and passwords.

    i. Vendor-supplied passwords are replaced. Review for generic, guest, and user IDs with unusual names. Ensure the appropriateness of these types of UNIX IDs.
2) Ensure that security software is restricted to security administrators.
3) Review UNIX users who have the ability to logon as superusers and determine whether this type of access is appropriate.
4) Review directory and file level permissions settings. Ensure that:
    a. Access to critical files, application source code file, databases, load libraries, security files, and operating system files is limited to those individuals requiring access.
    b. Appropriate access control software parameters are implemented.
    c. Access control software files are secured from unauthorized use.
    d. Access to the database management system (DBMS) software is controlled.
5) Ensure that access to job scheduling is secure. Review appropriateness of current automated jobs scheduled (i.e., commands that are to run according to a regular or periodic schedule; for example, a job will automatically run every night to back-up all critical files to tapes that will be shipped off-site).
6) Ensure that security features cannot be modified during start-up.

B. Ensure that database controls provide a secure environment for law enforcement data contained within the databases.
1) Determine whether the passwords for vendor-supplied user accounts have been changed. Examples include:
    a. INTERNAL – password ORACLE.
    b. SCOTT – password TIGER.
    c. SYSTEM – password MANAGER.
    d. SYS – password CHANGE_ON_INSTALL.
    e. DEMO – password DEMO.
    f. P08 – password P08.
2) Ensure that database user IDs are appropriately assigned.
    a. IDs are assigned to individual users and not to groups.
    b. Application users are not assigned multiple IDs.
    c. Operating System authenticated Oracle IDs are valid and current.
    d. DBMS owner ID and group are restricted to authorized system administration personnel and processes.
3) Review the Oracle user account profiles to ensure that password controls are implemented:
    a. Passwords must be changed every 30 to 90 days.
    b. Passwords must be at least six alphanumeric characters.
    c. Passwords may not be reused for at least 180 days (six generations).
    d. Three failed logon attempts lock out user ID.
4) In systems that grant users interactive database access through query tools and database tools (e.g., sqlplus and sqldba), ensure that user access is properly restricted through assignment of roles and privileges.

a. Ensure that the use of the DBMS utilities is limited.
b. Ensure that the UTL_FILE_DIR profile variable is configured appropriately.
5) Ensure that DBMS and data dictionary controls restrict access to application data (for selected systems) at the logical data view, field, or field-value level.
6) Ensure that access is controlled to the data dictionary (for selected systems).
7) Ensure that access to the security profiles in the data dictionary and security tables in the DBMS is limited.
8) Ensure that appropriate data dictionary and DBMS parameters are implemented.

C. Determine whether security support and operations job functions are performed by separate entities (i.e., job function).

4. Determine whether database administration for change control procedures is adequate by ascertaining whether the agency has instituted policies and implemented controls to ensure that all database modifications are properly authorized, tested and approved. Also, determine whether procedures are in effect to protect databases from unplanned system interruptions by ascertaining whether backup and recovery practices are properly in effect.

A. Ensure that database change control policies, procedures, and practices provide assurance that only authorized changes are made and implemented.
1) Identify the process used and authorizing officials for initiating, approving, testing, and implementing changes to the database.
2) Examine a sample of database changes for proper authorization and approval (for selected systems).
3) Determine whether a separation of duties exists for implementing changes to law enforcement data by ensuring that:
a. Application programmers do not have access to the production programs (for selected systems).
b. Application programmers cannot access operating system software.
c. Movement of programs and data (for selected systems) between libraries is controlled by an organization segment independent of both the user and programming staff.

B. Ensure that a security specialist reviews the changes to the database prior to the change to determine whether (and if so, how) changes will affect security.

C. Ensure that law enforcement data (for selected systems) can be restored in the event of an unplanned system interruption or when corruption of a database occurs.
1) Ensure that the agency Disaster Recovery Plan, Continuity of Operations Plan, and/or Business Resumption Plan provide for the ability to recover law enforcement data and provide service to meet the minimal needs of users of the system.
2) Review the contingency plan and compare its provisions with the most recent risk assessment and with current description of computer operations.
3) Ensure that the plan identifies all critical data files.

4) Ensure that a copy of a current contingency plan, which includes restoration of the database, is held off-site.
5) Ensure that plan reassessments are made as changes to the applications and databases supporting law enforcement data are conducted.
6) Ensure that plans that support the recovery of law enforcement data are tested and updated based on the test results.
7) Ensure that data and program back-up procedures exist and have been implemented.
    a. Ensure that written policies and procedures for backing-up the operating system, database, and application software exist. (Verify that all audit logs and data dictionary are part of the back-up procedure.)
    b. Ensure the adequacy of security and environmental controls at the back-up storage site.
    c. Ensure that database software being utilized is stored at an off-site location. Ensure that current data is being maintained by comparing inventory records with the database files (programs and data) maintained off-site and determining the age of these files.
    d. Ensure that the database administrator is responsible for planning the back-up and recovery of databases, and that data center personnel are responsible for routinely backing up files.
    e. Ensure that the agency has tested the recovery of the database using the back-up files.
    f. Ensure that security settings cannot be modified during the recovery start-up process.

D. Ensure that controls exist over data dictionary modifications, such as additions and deletions (for selected systems). At a minimum, identify the following:
   1) Ownership of the data dictionary.
   2) The person authorized to make changes to the data dictionary.
   3) Whether the most recent copy of the data dictionary is kept off-site for recovery purposes.
   4) How often it is updated.
   5) Whether old versions of the data dictionary are archived.

E. Ensure that the agency's standard naming conventions for its resources, such as database files, program libraries, individual programs, and applications, are implemented and that security controls cannot be bypassed (for selected systems).

F. Ensure that controls exist over database reorganization for selected systems (i.e., frequency based on volume, modifications, and deletions).

G. Ensure that database performance (for selected systems) is monitored and evaluated.
   1) Identify what maintenance is routinely performed on the database.
   2) Verify whether exception reports are utilized in monitoring and evaluating database performance.

5. Determine whether controls exist for remote users utilizing data and data distribution.

   A. Ensure that access controls exist over data contained on laptops and other portable devices (e.g., personal digital assistant) utilized by users.
      1. Ensure that there are policies and procedures regarding the protection of data contained on laptops and other portable devices.
      2. Ensure that the policies and procedures provide for:
         a. Data encryption.
         b. Data to be password protected.
         c. Utilizing the key lock on the laptop.
         d. The hard drive containing data to be removed when not in use and stored in a secure location.
         e. Data contained on CD-ROM to be encrypted and stored in a secure location when not in use.
   B. Determine whether the distribution of output, which includes data and sensitive reports, is controlled. Further, determine whether encrypted fax systems are used to send sensitive information.
   C. Verify that report listings from personnel management systems contain appropriate sensitivity identifiers.
   D. Determine whether the remote access configuration for the operating system deters unauthorized access.
      1) The /etc/hosts.equiv file and the .rhosts file in a user's home directory contain the names of remote hosts and users that are equivalent to the local host or user. An equivalent host or user is allowed to access a local non-superuser account without having to supply a password. Review these files for appropriateness.
      2) The /etc/services file associates Internet service names and aliases with the port number and protocol used by the service. Review each service running for appropriateness.
      3) The etc/inetd.conf and etc/inetd.conf.local files determine how to handle Internet service requests. Review for appropriateness.
      4) The UNIX-to-UNIX-Copy (UUCP) utility is a group of programs that enable you to connect to remote systems using a modem and telephone lines. Perform the following:
         a. Execute cat/usr/lib/uucp/Devices and document what ports and modem devices are set up for dialing out. Review for appropriateness.
         b. Execute cat/usr/lib/uucp/Systems and document. Review for appropriateness each remote system defined and what systems it is set up to call.
         c. Execute cat/usr/lib/uucp/Permissions to identify what permissions remote machines have with respect to login, file access, and command execution. Determine the appropriateness of the settings.
         d. Determine the appropriateness of the remote.unknown program setting (enabled or disabled), which is usually found in /usr/lib/uucp/remote.unknown.

E. Determine whether the remote access configuration for the Oracle database deters unauthorized access.
   1) Obtain the current parameter values (V$PARAMETER) and review the following:
      a. Determine appropriateness of protocols defined by MTS_LISTENER_ADDRESS.
      b. Determine whether Oracle is set to check passwords in the password file by reviewing REMOTE_LOGIN_PASSWORDFILE.
      c. Determine the appropriateness of allowing authentication of remote clients by reviewing REMOTE_OS_AUTHENT.
      d. Determine the appropriateness of allowing operating system roles for remote users by reviewing REMOTE_OS_ROLES.

Appendix K
Objectives for Evaluating UNIX Operating System Security

Overall Objective

The overall objective of this audit is to determine whether the agency has implemented controls to effectively manage UNIX operating system security.

Detailed Sub-Objectives

1. Determine whether system controls have been properly implemented. (**Note:** These steps will apply to all UNIX and Linux versions.)

   A. Assess whether the UNIX host is configurable and bootable in single-user mode, without a password.[97]
   B. Ensure that single-user mode incompatibility is documented.
   C. Verify whether a UNIX host that is not configured to require a password when booted to single-user mode is located in a controlled accessed area only by system administrators.[98]
   D. Determine whether UNIX system equipment is located in a controlled-access area.
   E. Determine whether the UNIX operating system version is a supported release.
   F. Assess whether vendor-recommended and security patches are installed and not out-of-date.
   G. Identify whether a system baseline was created and maintained.[99]
   H. Verify whether system baseline backups are stored on write-protected media.
   I. Determine the frequency of file systems checked for unauthorized system libraries or binaries or unauthorized modification to authorized system libraries or binaries.
   J. Identify whether a non-local/non-authoritative time server (protocol) is used.

2. Determine whether access controls have been properly implemented. (**Note:** These steps will apply to all UNIX and Linux versions.)

   A. Identify whether shared accounts are documented and justified.
   B. Verify whether a shared account is logged onto directly.
   C. Determine whether assigned accounts are unique.
      1) Ensure that accounts have not been assigned the same user identification (ID).
      2) Identify whether a user ID reserved for system accounts is used.

---

[97] A UNIX system is in a single-user mode when applications and third party software are not actively running. During this state, the system is vulnerable to configuration changes if a password is not present.
[98] An access-controlled area is defined as requiring two different checks of an individual's identity and authority before gaining access to the system.
[99] A system baseline includes cryptographic hashes of files in the baseline.

   3) Ensure that only the root user is assigned a user ID of 0.
- D. Identify whether all accounts with a Group ID (GID) of 99 and below (499 and below for Linux) are used by a system account. All groups should have an individual and unique GID.[100]
- E. Ensure that a group referenced in the /etc/passwd file is not in the /etc/group file.
- F. Verify that a logon banner is displayed prior to a logon attempt.
   1) Ensure that login banners are configured for all services that allow login access to the system.
   2) Identify whether the login banner contains the required notice and consent information.
- G. Verify that successful and unsuccessful logins and logouts are logged.
   1) Ensure that an account is disabled after three consecutive unsuccessful login attempts.
   2) Verify that the delay between login prompts after a failed login is set to at least four seconds.
   3) Identify whether the inactivity timeout/locking feature is configured for 15 minute intervals.
   4) Determine whether the UNIX system is running under continuous display mode.
- H. Assess the password controls that are used.
   1) Determine whether passwords can be changed once every 24 hours.
   2) Identify whether there are accounts with blank passwords.
   3) Verify that a password contains a minimum of 14 characters.
   4) Verify that a password contains at least 1 upper and 1 lower case alphabetic character, 1 numeric character, and 1 special character.
   5) Ensure that a password does not contain information.
   6) Assess whether passwords are changed every 60 days.
   7) Verify whether non-interactive/automated processing account passwords are changed.
   8) Identify whether an account is locked or disabled after 35 days of inactivity.
   9) Determine whether easily guessed passwords are used.
   10) Ensure passwords cannot be reused within the last 5 changes.
   11) Determine whether passwords are configured according to guidelines.
- I. Ensure that access to the root account is limited to security and administrative users and are documented.
- J. Verify whether administrative passwords are changed when an individual with access to the root password is reassigned.
- K. Identify whether the root account home directory has not been changed from '/'.
   1) Determine whether the root account home directory (other than '/') is more permissive than 700.

[100] Shared GID numbers could lead to undesirable file and directory access.

2) Identify whether the root account's search path contains a '.', '::', or starts or ends with a ':'.
3) Ensure that the root account has world writable directories in its search path.
4) Determine whether the root account can be directly logged into from somewhere other than the system console.
5) Verify whether remote consoles are defined.
6) Assess whether the root account is logged onto directly.
7) Verify whether successful and unsuccessful accesses to the root account are logged.
8) Verify whether the root shell is located in /usr, and /usr is partitioned.
9) Assess whether the root password is passed over a network in clear text form.
10) Perform the following to determine whether root has logged in over an unencrypted network connection:
    a) Determine whether root was logged in over a network.
    b) Check to ensure that Secure Shell (SSH) is installed.
11) Assess whether an encrypted remote access program, such as SSH, does not disable the capability to logon directly as root.

L. Assess whether there are files or directories with uneven access permissions.[101]
M. Identify whether there are unowned files.
N. Assess whether network services daemon files, the system command, and the library file are more permissive than 755.[102]
O. Ensure that system files, programs, and directories are owned by a system account and system group.
P. Verify whether the system log file is more permissive than 640.
Q. Verify whether the manual page file is more permissive than 644.
R. Assess whether NIS/NIS+/yp files are owned by root, sys, or bin.
    1) Verify that NIS/NIS+/yp files are not group-owned root, sys, bin, or other.
    2) Verify whether the NIS/NIS+/yp command file is more permissive than 755.
    3) Verify whether the /etc/passwd file is more permissive than 644.
    4) Verify that the /etc/passwd and /etc/shadow (or equivalent) file is not owned by root.
    5) Verify whether the /etc/shadow (or equivalent) file is more permissive than 400.
S. Determine whether a home directory defined in the /etc/passwd file exists.
    1) Determine whether users are assigned a home directory in the /etc/passwd file.
    2) Verify whether the user home directory(s) is more permissive than 750.
    3) Verify whether the user home directories contain files/directories more permissive than 750.
    4) Verify whether users own their home directory.

[101] Uneven file permission exists if the file owner has less privileges than the group or world users, and when the file is owned by a privileged user or group (such as root or bin).
[102] In multitasking computer operating systems, a daemon is a computer program that runs as a background process, rather than being under the direct control of an interactive user.

5) Verify whether home directories are group-owned by the home directory owner or primary group.
6) Assess whether user home directories contain files/directories owned by the home directory owner.

3. Determine whether general controls have been properly implemented. (**Note:** These steps will apply to all UNIX and Linux versions.)

A. Verify whether the NIS protocol is used while the NIS+ protocol is available.
B. Determine whether NIS/NIS+ is implemented under User Datagram Protocol.
C. Identify whether NIS maps are protected through hard-to-guess domain names.
D. Determine whether the NIS+ server is operating at security level 2.
E. Assess whether the .rhosts, .shosts, hosts.equiv, or shosts.equiv are used, not justified, and documented with the Information Assurance Officer (IAO).
F. Identify whether the shell files have the suid bit set.
G. Identify whether the finger service is enabled.
H. Evaluate whether Anonymous File Transfer Protocol (FTP) has been configured using all security recommendations.
I. Identify whether FSP is enabled.
J. Determine whether the Trivial File Transfer Protocol (TFTP) daemon is running in secure mode.
   1) Identify whether the TFTP daemon has the suid or sgid bit set.
   2) Assess whether TFTP is active.
   3) Verify whether TFTP that is active is justified and documented with the IAO.
K. Identify whether a system is exporting X displays to the world.
L. Ensure that the Simple Network Management Protocol (SNMP) community strings have been changed from the default.
M. Identify whether remote login or remote shell is enabled.
N. Identify whether the rexec service is enabled.
O. Assess whether an audio device is:
   1) More permissive than 644.
   2) Not owned by root.
   3) Not group-owned by root, sys, bin, or audio.
P. Identify whether the ownership, permissions, and location of files with the suid bit set are documented with the IAO.
   1) Assess whether the system is checked weekly against the system baseline for unauthorized suid files as well as unauthorized modification to authorized suid files.
   2) Identify whether the user file systems, removable media, or remote file systems are mounted with the nosuid option invoked.
   3) Identify whether the ownership, permissions, and location of files with the sgid bit set are documented with the IAO.

4) Assess whether the system is checked weekly against the system baseline for unauthorized sgid files as well as unauthorized modification to authorized sgid files.

Q. Determine whether the public directories are not owned by root or an application user.

R. Ensure that the public directories are not group-owned by root, sys, bin, other or an application group.

S. Evaluate whether development systems are subject to the same security requirements as production systems.

T. Ensure that default accounts have been disabled.

U. Determine whether access to the cron utility is controlled via the cron.allow and/or cron.deny file(s).[103]
   1) Identify whether the cron.allow file is more permissive than 600.
   2) Evaluate whether cron executes group or world writable programs.
   3) Assess whether cron executes programs in or subordinate to world writable directories.
   4) Ensure that the crontabs are owned by root or the crontab creator.
   5) Identify whether the default system accounts (with the possible exception of root) are listed in the cron.allow file or excluded from the cron.deny file if cron.allow does not exist.
   6) Identify whether the crontab files are more permissive than 600 (700 for some Linux files).
   7) Identify whether the cron or crontab directories are more permissive than 755.
   8) Ensure that the cron or crontab directories are not owned by root or bin.
   9) Ensure that the cron or crontab directories are group-owned by root, sys, or bin.
   10) Verify whether cron logging is implemented.
      a. Assess whether the cronlog file is more permissive than 600.
      b. Assess whether the cron.deny file is more permissive than 700.
      c. Identify whether the cron.allow file is not owned and group-owned by root, sys or bin.
      d. Identify whether the cron.deny file is not owned and group-owned by root, sys, or bin.

V. Determine whether access to the at utility is controlled via the at.allow and/or at.deny file(s).
   1) Identify whether the at.deny file exists and is empty.
   2) Ensure that the default system accounts (with the exception of root) are listed in the at.allow file or excluded from the at.deny file if at.allow does not exist.
   3) Assess whether the at.allow or at.deny file(s) is more permissive than 600.
   4) Identify whether the at executes group or world writable programs.
   5) Identify whether the at executes programs in or subordinate to world writable directories.

[103] The cron utility is the time-based job scheduler in Unix-like computer operating systems. Cron enables users to schedule jobs (commands or shell scripts) to run periodically at certain times or dates.

6) Assess whether the at (or equivalent) directory is more permissive than 755.
7) Ensure that the at directory is not owned by root, sys, bin, or daemon.

W. Determine whether there are any at jobs by viewing a long listing of the directory. If there are at jobs, perform the following to check for any programs that may have an unmask more permissive than 077:
   1) Assess whether the at.allow file is not owned and group-owned by root, sys, or bin.
   2) Identify whether the at.deny file is not owned and group-owned by root, sys, or bin.
   3) Evaluate whether the executable stack is disabled.

X. Determine whether random Transmission Control Protocol sequence numbers are used.

Y. Evaluate whether network parameters are securely set.

Z. Identify whether logging is implemented for the root file system.

AA. Determine whether authentication and informational data is logged.

BB. Determine whether the run control scripts execute world writable programs or scripts. Also:
   1) Identify whether the run control scripts are more permissive than 755.
   2) Determine whether the run control scripts PATH variable contains a '.' or a '::', or starts or ends with a '.'.
   3) Evaluate whether the run control scripts have the sgid or the suid bit set.
   4) Ensure that the run control scripts are not owned by root or bin.
   5) Ensure that the run control scripts are not group-owned by root, sys, bin, other or the system default.
   6) Evaluate whether the run control scripts execute programs owned by neither a system account nor an application account.

CC. Assess whether the global initialization files are more permissive than 644.
   1) Ensure that global initialization files are not owned by root.
   2) Ensure that global initialization files are not group-owned by root, sys, bin, other, or the system default.
   3) Determine whether the global initialization files PATH variable contains a '.' or a '::', or starts or ends with a ':'.
   4) Identify whether the global initialization files contain the command mesg –n.

DD. Assess whether the default skeleton '.' files are more permissive than 644.

EE. Ensure that the default skeleton '.' files are not owned by root or bin.

FF. Identify whether the local initialization files are owned by the user or root.
   1) Assess whether the local initialization files are more permissive than 740.
   2) Determine whether the local initialization files PATH variable contains a '.' or a '::', or starts with a '.'.
   3) Identify whether the local initialization files have the suid or the sgid bit set.
   4) Determine whether the local initialization files execute world writable programs or scripts.
   5) Identify whether the local initialization files contain the mesg -y or mesg y command.

GG. Evaluate whether the .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow, and/or /etc/group files contain a plus (+) and define entries for NIS+ netgroups.
1) Identify whether an A .netrc file exists.
2) Determine whether the .rhosts, .shosts, hosts.equiv, or shosts.equiv files contain other than hostname-user pairs, are justified, and documented with the IAO.
3) Identify whether the .rhosts, .shosts, hosts.equiv, shosts.equiv, or .netrc files are accessible by users other than root or the owner.
4) Evaluate whether the .rhosts file is supported in PAM.
5) Determine whether the /etc/shells (or equivalent) file does not exist.
6) Identify whether the A shell referenced in /etc/passwd is not listed in the shells file.
7) Determine whether the shell files have the sgid bit set.
8) Identify whether shell files are owned by root or bin.
9) Assess whether the shell files are more permissive than 755.

HH. Determine whether the device file directories are writable by users other than a system account or as configured by the vendor.

II. Identify whether the device files used for backup are writable by users other than root or a pseudo backup user.

JJ. Assess whether the Network File System(NFS) exported system files and system directories are not owned by root. Evaluate whether:
1) The NFS server is configured to deny client access requests that do not include a userid.
2) The NFS server is configured to restrict file system access to local hosts
3) The sec option is set to none (or equivalent); additionally the default authentication is set to none.
4) The root access option for NFS has been justified and documented with the IAO.
5) The nosuid and nosgid options are not enabled on a NFS Client.
6) NFS file systems exported as writable have been justified and documented by the IAO.

KK. Identify whether a public instant messaging client is installed.

LL. Identify whether a peer-to-peer file-sharing application is installed and, if so, ensure that it is authorized and documented with the designated accreditation authority.

MM. Evaluate whether Samba is running and is not operationally required.

NN. Determine whether the Samba Web Administration tool is not used with SSH port-forwarding.

OO. Determine whether network analysis tools are enabled.

PP. Determine whether the /etc/server message block (smb).conf file is:
1) Not owned by root.
2) Not group-owned by root.
3) More permissive than 644.

QQ. Determine whether the /etc/samba/smbpasswd file is:
1) Not owned by root.

2) Not group owned by root.
3) More permissive than 600.

RR. Determine whether the smb.conf file is not configured to:
1) Set the hosts allow option to contain only the local network subnet masks and the loopback address.
2) Set the security option to user.
3) Set the encrypt passwords option to yes.
4) Enter the path to the smbpasswd utility in the smb password file option.

SS. Ensure that all guest entries in the shares definition section of the smb.conf file are set to no.

TT. Identify whether an Internet network news server is justified and documented by the IAO.
1) Assess whether the /etc/news/hosts.nntp file is more permissive than 600.
2) Assess whether the /etc/news/hosts.nntp.nolimit file is more permissive than 600.

UU. Identify whether the system is a print server/client, and the configuration is documented with the IAO.
1) Assess whether the /etc/news/nnrp.access file is more permissive than 600.
2) Assess whether the /etc/news/passwd.nntp file is more permissive than 600.
3) Determine whether the files contained in the /etc/news directory are not owned by root or news.
4) Determine whether the files contained in the /etc/news directory are not group-owned by root or news.

VV. Identify whether the hosts.lpd file (or equivalent) contains a '+' or '_' character.
1) Assess whether the hosts.lpd (or equivalent) file is not owned by a root, sys, bin, or lp.
2) Assess whether the hosts.lpd (or equivalent) file is more permissive than 664.

WW. Identify whether the traceroute command is not owned by root.
1) Ensure that the traceroute command is not group owned by root, sys, or bin.
2) Assess whether the traceroute command is more permissive than 700.

XX. Determine whether all inetd/xinetd services are disabled, and inetd (xinetd for Linux) is not disabled.
1) Assess whether the inetd.conf (xinetd.conf for Linux) file is more permissive than 440.
2) Identify whether the Linux xinetd.d. directory is more permissive than 755.

YY. Determine whether the services file is not owned by root or bin.

ZZ. Ensure that the ftpusers file does not exist
1) Assess whether the ftpusers file contains account names not allowed to use FTP.
2) Identify whether the ftpusers file are not owned by root.
3) Assess whether the ftpusers file is more permissive than 640.
4) Assess whether the services file is more permissive than 644.
5) Determine whether the FTP daemon is configured for logging or verbose mode.
6) Identify whether there is an anonymous FTP account with a functional shell.

7) Ensure that an FTP user's unmask is not 077.

AAA. Determine whether TFTP is configured to vendor specifications, including the following:
1) A TFTP user will be created.
2) The default shell will be set /bin/false, or equivalent.
3) A home directory owned by the TFTP user will be created.

BBB. Determine whether an X Windows host writes .Xauthority files (or equivalent).
1) Identify whether Xauthority files are more permissive than 600.
2) Evaluate whether authorized X clients are not listed in the X*.hosts (or equivalent) file(s) if the .Xauthority utility is not used.
3) Ensure that an authorized X clients are not listed in the X*.hosts (or equivalent) file(s) if the .Xauthority utility is not used.
4) Assess whether the X window system connections are not required, but the connections are not disabled.

CCC. Identify whether the Unix-to-Unix Copy service is enabled.

DDD. Identify whether the snmpd.conf file is more permissive than 700.

EEE. Assess whether the management information base (mib) files are more permissive than 640.

FFF. Identify whether the snmpd.conf and .mib files are not owned by root and group-owned by sys or the application.

GGG. Identify whether SNMP runs on dedicated hardware.

HHH. Determine whether SSH, or a similar utility, is running and SSHv1 compatibility is used.

III. Evaluate whether encrypted communications are configured for Internet Protocol (IP) filtering and logon warning banners.

JJJ. Ensure that the system is not a router and has no defined default gateway.
1) Identify whether a system used for routing also uses other applications and/or utilities.
2) Determine whether IP-forwarding is disabled.

KKK. Assess whether a system running Squid Web Proxy Cache is vulnerable to the MSNT auth helper buffer overflow exploit.

LLL. Identify whether NFS port monitoring is enabled.

MMM. Determine whether the export configuration file is owned by root.

NNN. To determine whether the NIS protocol is in use and not justified and documented with the IAO.

OOO. Identify whether there is a host-based intrusion detection tool.

PPP. Identify whether a system vulnerability assessment tool is being run on the system monthly.

QQQ. Verify whether the system vulnerability assessment tool, host-based intrusion detection tool, and file system integrity baseline tool notify the systems administrator and the information awareness office of a security breach or a suspected security breach.

RRR. Identify whether an access control program is being used.
1) Determine whether the access control program logs each system access attempt.

2) Assess whether the access control program is configured to grant or deny system access to specific hosts.

SSS. Identify whether an approved virus scan program is used and updated.

1) Check for the existence of the MacAfee command line scan tool to be executed weekly in the cron file.[104]
2) Ensure that the definitions file is not older than 14 days.

TTT. Identify whether the sticky bit is set on public directories.

UUU. Ensure that the system and user default unmask are not 077.

1) Assess whether the applications requiring an unmask more permissive than 077 are justified and documented with the IAO.
2) Assess whether the Cron programs requiring an unmask more permissive than 077 are justified and documented with the IAO.

VVV. Identify whether core dumps are disabled.

WWW. Ensure that the core dump data directory is not owned or group-owned by root or is more permissive than 700.

XXX. Evaluate whether separate file system partitions are used for /home, /export/home, and /var and are justified and documented with the IAO.

YYY. Determine whether the system is checked weekly against the system baseline for extraneous device files.

ZZZ. Evaluate whether network services required for operations are not disabled or documented with the IAO.

AAAA. Ensure that the inetd.conf file (xinetd.conf file and the xinetd.d directory for Linux) is not owned by root or bin.

BBBB. Determine whether Inetd (xinetd for Linux) logging/tracing is enabled.

CCCC. Determine whether a Lotus Domino 5.0.5 Web Application was found vulnerable to the .nsf, .box, and .ns4 directory traversal exploit.

DDDD. Evaluate whether a system running Squid Web Proxy Cache server is vulnerable to the authentication header forwarding exploit. If so, verify whether the systems administrator will ensure the Squid Proxy Cache server is not a vulnerable version.

EEEE. Determine whether an iPlanet web server was found with the search engine NS-query-pat file viewing vulnerability.

FFFF. Identify whether the export configuration file is more permissive than 644.

4. Determine whether audit log controls have been properly implemented. (**Note:** These steps will apply to all UNIX and Linux versions.)

   A. Identify whether auditing is implemented.
   B. Ensure that unauthorized users cannot access system audit logs.
   C. Assess whether system audit logs are more permissive than 640.

[104] The MacAfee command line scanner is available for most Unix/Linux operating systems. Additional tools specific for each operating system are also available and will have to be manually reviewed if they are installed.

D. Identify whether the audit system is configured to audit the following:
   1) Failed attempts to access files and programs.
   2) Files and programs deleted by the user.
   3) All administrative, privileged, and security actions.
   4) Login, logout, and session initiation.
   5) All discretionary access control permission modifications.
E. Identify whether audit logs are rotated daily.
F. Determine whether audit data is retained for at least 1 year or synchronized accessible media interchange audit data is retained for 5 years.
G. Assess whether audit data is backed up onto a different system or backup media on at least a weekly basis.
H. Determine whether the audit trails and/or system logs are reviewed on a daily basis for:
   1) Excessive logon attempt failures by single or multiple users.
   2) Logons at unusual/non-duty hours.
   3) Failed attempts to access restricted system or data files indicating a possible pattern of deliberate browsing.
   4) Unusual or unauthorized activity by system administrators.
   5) Command-line activity by a user that should not have that capability.
   6) System failures or errors.
   7) Unusual or suspicious patterns of activity.
I. Ensure that the /etc/syslog.conf file is not owned by root or is more permissive than 640.
J. Ensure that the /etc/syslog.conf file is not group owned by root, sys, or bin.
K. Identify whether local hosts are used as loghosts for systems outside the local network.
L. Ensure that a system using a remote loghost is not documented with the IAO.
M. Verify that the syslog daemon accepts remote messages and is not an IAO-documented loghost.

Appendix L
Objectives for Evaluating Remote Access Controls and Security

Overall Objective
The overall objective of this audit is to determine whether the agency has provided system security, integrity, and control over remote access to its computer systems and data.[105]

Detailed Sub-Objectives

1. Evaluate whether the agency has developed adequate security policies and procedures for granting and controlling remote access to system resources through a Virtual Private Network (VPN).
   A. Assess whether VPN firewalls: Deny and log all services not expressly permitted.
      2) Audit and monitor all services.
      3) Stop passing packets if logging is disabled.
      4) Do not implement the Dynamic Host Configuration Protocol service.
      5) Implement and authenticate Network Time Protocol.
      6) Employ current operating system versions.
      7) Log sufficient activity to facilitate forensic analysis.
      8) Authenticate route updates using the MD5 hashing algorithm.
      9) Implement session timeouts of at most # minutes.
      10) Modified the Simple Network Management Protocol community strings (passwords) from their default values.
      11) Mitigate denial of service.
      12) Back-up logs for at least 1 year or as directed by the records office.
      13) Use encrypted connections to access the firewalls.
   B. Analyze whether VPN controls comply with agency policy or best practices:
      1) Ensure that all remote access users have unique user identifications, passwords comply with complexity requirements, and two-factor authentication is used according to Payment Card Industry standards.
      2) Allow the lowest level of encryption the server will negotiate, ensuring that minimum required encryption standards are enforced (Advanced Encryption Service/Triple Data Encryption Standard).
      3) Ensure that client-side software prohibits split tunnels.
      4) Enable client workstation security to address the following:
         a. Client workstations that do not meet security requirements are quarantined or blocked.
         b. Determine whether traces of session information are left on remote computer after session termination (servers push software to clear client cache).

[105] References to "agency" apply to any responsible office, component, or governing body.

c. Limit non-ACE client's network access and perform client configuration checks.[106]

5) Ensure that warning banners are displayed prior to logon.
6) Ensure that only ACE workstations have unrestricted access to the agency network.
7) Determine whether users are restricted to a specific set of applications through WebVPN.
8) Ensure that restricted access is provided through an indirect, secure mechanism.
9) Determine whether aggressive mode is required for authentication purposes. (**Note:** Used only for Internet Protocol [IP] Security.)
   a. If not required, it should be disabled at the server (Cisco configuration parameter).
   b. If it is required, then:
      i. Ensure that digital certificates or other two-factor authentication methods are used.
      ii. Ensure that the use of pre-shared keys is prohibited.
10) Determine whether VPN infrastructure devices/servers are patched and have the current operating system.
11) Determine whether the operating system is configured to limit services, and has antivirus and all current patches installed.

C. Determine whether management approval controls comply with agency policy or best practices:
   1) Ensure that management controls align with agency policy or best practices.
   2) Employ statistical sampling to make conclusions regarding user population.
   3) Ensure that the samples of remote access users for each environment are still active employees.
   4) Ensure that when user accounts are disabled in Active Directory, access is revoked.
   5) Ensure that electronic access approvals were obtained for each user in the sample.
   6) Ensure that all users have attended security awareness training or user acceptance training prior to obtaining access to remote access environment.

2. Determine whether the agency maintains a computer incident database and whether information stored within the computer incident tracking database is sufficiently reliable.

   A. Data Attribute Definition – define the data attributes and expected values of the computer incident tracking database to determine attributes for testing.
   B. Data Identifiers – for the attributes defined above, determine whether invalid or duplicate identifiers exist in the computer incident tracking database.
   C. Duplicate Records – determine whether duplicate records exist in the computer incident tracking database.

[106] ACE is an embeddable code editor written in JavaScript. It matches the features and performance of native editors such as Sublime, Vim, and TextMate.

   D. Missing Data – for the attributes defined above, determine whether missing data values or records exist in the computer incident tracking database.
   E. Data Values – for the attributes defined above, determine whether the computer incident tracking system contains data values outside of the designated range.
   F. Timeliness – for the attributes defined above, determine whether the incident dates are within valid time periods and follow a logical progression.
   G. Data Validation and Edit Checks – determine whether data validation and edit checks exist and work as intended.
   H. Completeness Testing – select a judgmental sample of incident tickets and trace the tickets to the record set to determine whether record sets are complete.
   I. Gap Analysis – determine whether the structure of the incident database follows industry suggested practices.

3. Determine whether the security controls over the agency's public-facing web infrastructure adequately protect the agency applications and data.

   A. Agency Documented Web Servers – determine the IP addresses, Fully Qualified Domain Name (FQDN), location, and responsible personnel for all agency public-facing web servers.

      1) Obtain a list from the agency of IP addresses belonging to public-facing web servers.
      2) Request the FQDN for the servers.
      3) Determine which web servers belong to which application(s).
      4) Determine responsible personnel for each group of applications or each web server and obtain a point of contact.
      5) Query agency business owners to determine whether there are additional public-facing web servers in the environment that do not fall under the responsibility of the information technology department.

   B. Office of Inspector General (OIG) Discovery – determine the IP addresses for all agency public-facing web servers through OIG scanning tools.
      1) Use a scanning tool to perform discovery on the agency's network environment.
      2) If necessary, perform a scan using Nmap to determine the environment.
      3) Identify all public-facing web servers belonging to the respective domains known by Google.
      4) Analyze results to determine IP addresses, server name, locations, and hosts that belong to all agency public-facing web servers.
   C. Test Plan
      1) Gather information related to applications for web server sample.
      2) Determine the criticality rating and key contact personnel for each application within the audit scope.
      3) Gather background information for the applications within the audit sample.
      4) Schedule meetings with key personnel for each application.
      5) Determine any scope limitations and document the sample.
   D. UNIX Systems

1) Using the scan results from scanning software, such as GFI Languard and Nessus, determine whether the UNIX operating systems are consistently patched and configured in accordance with agency policy or best practices.
2) Using the scan results, determine whether UNIX system accounts:
    a. Store passwords in one-way encrypted format.
    b. Have enabled password shadowing.
    c. Have a minimum password length of # characters.
    d. Have enabled password quality checking to meet policy.
    e. Are subject to password aging on all accounts.
    f. Have a minimum password age of at least 1 day.
    g. Enable account lock-outs after # failed logon attempts.
    h. Automatically suspended after the required maximum number of unsuccessful logon attempts.
3) Using the scan results, determine whether UNIX system file system security:
    a. Uses “no s-uid” Option for non-system partitions.
    b. Disables user-mounted removable file systems.
    c. Configures /var on its own partition.
4) Using the scan results, determine whether the UNIX server has the current patches installed.
5) Using the scan results, determine whether the UNIX server has:
    a. Set password expiration on active accounts.
    b. No accounts with empty password fields.
    c. No user identification 0 accounts other than root.
    d. Eliminate root path containing current directory.
    e. Forbid root to logon remotely.
    f. Set root's umask.
    g. Eliminate the use or R commands.
    h. Restrict Ability to run su.
    i. Create an approved security message.
    j. Establish console timed lockout.
6) Using the scan results, determine whether the UNIX server has:
    a. Configured Transmission Control Protocol wrappers to limit access.
    b. Disabled File Transfer Protocol.
    c. Disabled rlogin/rsh/rcp.
    d. Disabled Trivial File Transfer Protocol server.
    e. Disabled Kerberized rlogin.
    f. Disabled rquotad.
    g. Disabled Common Desktop Environment related daemons.
    h. Disabled inetd.
    i. Disabled E-mail server.
    j. Disabled Network Information Service Client/Server.
    k. Disabled Network File System Client/Server.

l. Disabled graphical user interface logon.
m. Disabled services that are not commonly used.
n. Set network configuration settings.
o. Disabled unnecessary services and daemons.
p. Disabled Secure Sockets Layer/Transport Layer Security Server Support For Weak Cipher Algorithm.
q. Disabled telnet service.
r. Disabled the use of xhost.

7) Configurations for necessary services:
   a. Ensure that OpenSSH is up-to-date.
   b. Eliminate Anonymous File Transfer Protocol.
8) Console Security: Set Password on the Grand Unified Bootloader.

E. Windows Systems
   1) Using the scan results from scanning software, such as GFI Languard and Nessus, determine whether if the Windows operating systems are consistently patched and configured in accordance with agency policy or best practices.
   2) Using the scan results, determine whether Windows Local Server passwords has:
      a. Enforced password history.
      b. Maximum password age.
      c. Minimum password age.
      d. Minimum password length.
      e. Complexity requirements in accordance with policy.
      f. Account lockout duration.
      g. Account lockout threshold.
      h. Default accounts locked or have their passwords changed from the default values.
   3) Using the scan results, determine whether Windows local server has the current patches installed, including:
      a. Microsoft service pack level.
      b. Required hot fixes and security updates.
      c. Non-operating system patches, hot fixes, and security updates.
   4) Using the scan results, determine if the antivirus and Intrusion Prevention Software is up-to-date as required by policy.

F. Using scan results from scanning software, such as Hewlett Packard WebInspect, determine whether the web server has:
   1) Current patches installed as required by policy.
   2) Passwords that meet agency standards.
   3) Fields subject to injection flaws.
   4) Authentication and session management vulnerabilities.
   5) Insecure direct object references.
   6) Cross-site request forgery.
   7) Insecure cryptographic storage.

8) Fail to restrict Uniform Resource Locator access.
9) Insufficient transport layer protection.
10) Un-validated redirects and forwards.
11) Cross-site scripting.

Appendix M
Objectives for Evaluating Mobile Device Security

Overall Objective
The overall objective of this audit is to determine the effectiveness of agency efforts to safeguard sensitive information stored or processed on mobile devices.[107]

Detailed Sub-Objectives

1. Determine whether the agency and its components have developed adequate policies and procedures to protect the data processed and stored on mobile devices.

   A. Evaluate whether the agency and its components have established policies and procedures to safeguard and restrict the use of mobile devices and that procedures developed are aligned with Office of Management and Budget and National Institute of Standards and Technology policy.
   B. Assess whether authorized mobile devices are marked to protect information stored from mishandling.

2. Determine whether the agency and its components maintain an accurate inventory of mobile devices.

   A. Identify the processes used by the agency to inventory, assign, and dispose of mobile devices.
      1) Identify whether management of the devices is centralized.
      2) Identify any third party software being used to centrally manage and deploy mobile device software (i.e., Apple) in the agency enterprise.
      3) Determine whether there is a specific program/application used for administration of settings on mobile devices.
      4) Determine whether the device acquisition chain (i.e., supply chain) is vetted before government use.
      5) Determine how devices are secured while in transit or at rest.
   B. Review and compare the inventory to the number of mobile devices listed in the equipment database and trace information such as make, model, and serial number to the equipment database.
   C. Analyze the agency's controls to ensure that mobile devices are sanitized and disposed in accordance with applicable procedures.
   D. Evaluate the agency's process for reporting security incidents involving mobile devices and sample reported events regarding lost or damaged devices.

[107] References to "agency" apply to any responsible office, component, or governing body.

E. Ensure that stolen and missing mobile devices are reported within the established timeframe.

3. Determine the effectiveness of controls implemented to protect the data stored and processed on mobile devices that connect to the agency's network(s).

   A. Assess the encryption settings used to secure agency data, both in transit and stored, when applicable.
      1) Determine whether the device uses local encryption when data is at rest (Data-at-Rest).
         a. Identify specifics on where the local device is encrypted, (i.e., local hard drive, software, boot sector, Virtual Private Network).
         b. Determine whether the device is compliant with Federal Information Processing Standards (FIPS) 140-2.
         c. Identify the algorithm used (i.e., Advanced Encryption Standard [AES]).
         d. Determine whether the device is compliant with agency requirements on encryption (e.g., AES-256).
      2) Determine whether the device uses encryption technologies when data is in transit (Data-in-Transit).
         a. Determine whether the device is FIPS 140-2 compliant.
         b. Identify the algorithm used.
         c. Determine whether the device is compliant with agency requirements on encryption.
         d. Identify whether wireless fidelity (Wi-Fi) is enabled on the device to connect to an agency network. If yes, determine whether the device requires/is capable of Wi-Fi Protected Access-2.
   B. Determine whether mobile device users are connecting to the enterprise network via a secure connection (Virtual Private Network, Internet Protocol security, or Secure Sockets Layer.
   C. Identify and evaluate the configuration management controls for mobile devices connected to third-party applications, local networks, and back-end servers, to ensure that settings comply with agency policies and procedures.
      1) Identify the common configuration management controls implemented on the agency's mobile devices. For example:
         a. User authentication (e.g., two-factor authentication - PIN and RSA token). Identify whether user authentication is required on "power-on."
         b. Antivirus software (i.e., AVG, Lookout, or Norton Security). Verify enterprise updates to the mobile device antivirus software to prevent the perpetuation of malware.
         c. Access to camera and video recording functions.
         d. Enabling of audit log functions.
      2) Determine whether users can save agency data/files to local mobile devices.

3) Determine whether mobile devices are set to lock automatically after a specified amount of time.
4) Identify whether devices are wiped after a specific number of failed login attempts.
5) Determine whether users can download and install applications to a device. If so, identify whether applications are vetted before they can be download onto agency mobile devices.
6) Identify whether there are any location based services being used, allowed, or required to track mobile devices. If so, determine whether the mobile devices are being tracked or monitored in any way (e.g., remote lockdown, erase, or track).
7) Identify whether role-based permissions are assigned to the mobile device user/mobile device.
8) Determine whether the devices authorized for use on the agency's network are government owned or employee (i.e., personally) owned.
9) Identify whether device authorization is at the device level (Media Access Control address).
10) Determine how often the agency/component synchronizes and backs-up all stored information.

D. Evaluate the frequency of discovery scans performed for thumb drives, tablets, and smartphones to identify whether unauthorized mobile devices are being connected to the agency's network(s).
1) Determine whether mobile devices are scanned in any way to help prevent the spread of malware, viruses, or known vulnerabilities (i.e., installation of AVG, Lookout, or Norton Security).
2) Identify how often servers are scanned to find unauthorized Universal Serial Bus connections.
3) Identify the patching process for application and mobile device operating systems.
4) In cases where the agency does not push out security updates/patches, determine how often vendor-related or security vulnerability alert sites are monitored.
5) Determine how unauthorized portable devices are reported to management.

E. Identify the risks associated with mobile devices that could affect the safeguarding and protection of agency and other sensitive data.
1) Ensure that agency management's acceptance of risks, such as privacy risks, is documented.
2) Analyze any weaknesses or deficiencies listed on a Plan of Action and Milestones for portable devices.

F. Determine how the agency is addressing the additional risk of users accessing personal social media sites and banking services while using the mobile device for official use.

4. Verify and evaluate the agency awareness program that addresses the importance of securing the mobile devices physically and logically. Ensure that the training includes the types of information that can and cannot be stored on such devices.

Appendix N
Objectives for Evaluating Portable Storage Device Security

Overall Objective
The overall objective of this audit is to determine whether the agency has addressed the emerging threat of theft and mishandling of sensitive and classified information as a result of the proliferation of portable storage devices through policy and security controls.[108]

Detailed Sub-Objectives

1. Determine whether the agency has developed adequate policies and procedures to protect the data processed and stored on the portable devices.

   A. Evaluate whether the agency has established policies and procedures to safeguard and restrict the use of portable devices and ensure procedures developed are aligned with Office of Management and Budget and National Institute of Standards and Technology policy.
   B. Assess that authorized portable devices are properly marked to protect information stored from mishandling.

2. Determine whether the agency maintains an accurate inventory of portable devices.

   A. Identify the processes used by the agency to inventory, assign, and dispose of portable devices.
   B. Review and compare inventory to the number of portable devices listed in the equipment database and trace information such as make, model, and serial number to the equipment database.
   C. Analyze the agency's controls to ensure portable devices are sanitized and disposed in accordance with applicable procedures.
   D. Evaluate the agency's process for reporting security incidents on portable devices and sample reported events regarding lost or damaged portable devices.
   E. Ensure that stolen and missing portable devices are reported within the established timeframe.

3. Determine the effectiveness of controls implemented to protect the data stored and processed on portable devices that connect to the agency's networks.

   A. Assess encryption settings used to secure agency data, both in transit and stored, when applicable.

[108] References to "agency" apply to any responsible office, component, or governing body.

B. Review configuration management controls for portable devices connected to third-party applications, local networks, and back-end servers, to ensure that settings comply with the agency's policies and procedures.
C. Evaluate the agency's frequency of discovery scans performed for thumb drives, tablets, and smartphones to identify whether unauthorized portable devices were connected to the agency's network.
D. Identify risks associated with portable devices that could affect the safeguarding or protection of agency data.

Appendix O
Objectives for Evaluating E-mail Security

Overall Objective
The overall objective of this audit is to determine the adequacy of agency security controls designed for E-mail services to ensure the confidentiality, availability, and integrity of sensitive information.[109]

Detailed Sub-Objectives

1. Obtain background information on the agency's E-mail services.

   A. Review appropriate criteria, regulations, guidelines, and recent publications relevant to E-mail security.
   B. Obtain an understanding of the agency's E-mail and general system maintenance practices.
   C. Evaluate the agency's internal policies and procedures regarding E-mail appropriate use for sensitive material and general retention guidelines (e.g., back-up, restoration, archiving procedures).
   D. Evaluate whether E-mail administrators have a process to enforce and monitor compliance with policy.
   E. Evaluate whether the annual E-mail security awareness training is satisfactory.

2. Secure E-mail infrastructure: Determine whether the agency has considered the various risks associated with E-mail and taken appropriate actions to harden its E-mail infrastructure against known attacks.

   A. Determine what security precautions were taken during the design of the E-mail infrastructure.
   B. Ensure that a risk assessment was performed.
   C. Evaluate whether the operating system was hardened. Determine whether any Windows security templates were used.
   D. Determine whether allowed services were identified.
   E. Obtain an overall diagram of the agency's E-mail infrastructure. As necessary, develop tests over E-mail components, particularly those that are Internet facing.
   F. Scan a sample of servers for configuration settings and compare to policy and the agency's baseline configuration.
   G. Identify servers responding to Simple Mail Transfer Protocol (Port 25). Test for unauthorized servers running mail services.

[109] References to "agency" apply to any responsible office, component, or governing body.

3. Determine how changes are introduced to the production E-mail infrastructure.

   A. Testing in this section involves reviewing access privileges for introducing change. On the Windows environment, Short Message Service is the primary delivery mechanism. For example, ensure that changes to mail routing and other mail options are controlled.
   B. Identify controls that would prevent a local area network administrator from intercepting and reading the E-mail of another individual.
   C. Determine what controls exist over Public Folders within Exchange.
      1) Review how security permissions are made for the folder.
      2) Determine how Windows Distribution groups are identified, organized, and disseminated to different groups.
      3) Identify how business owners are involved.

4. Determine whether the agency's encryption policy is adequate. Ensure that necessary controls are in place over encrypted E-mail.

5. Determine whether necessary controls exist for the physical security of the E-mail infrastructure.

6. Confirm whether the organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

   A. Determine whether the agency uses any third-party tools to maintain or support its exchange infrastructure.
   B. Determine what virus scanning software or spam filtering software is installed on the exchange servers to scrub E-mails.
   C. Determine whether the agency has documented maintenance procedures for its exchange infrastructure.
   D. Determine whether the following controls are in place (whether maintenance is performed from remote locations for any of the platforms being reviewed):
      1) The agency approves, controls, and monitors remotely executed maintenance and diagnostic activities.
      2) The agency maintains maintenance logs for all remote maintenance, diagnostic, and service activities.
      3) Appropriate agency officials periodically review maintenance logs.
      4) When remote maintenance is completed, the agency (or information system in certain cases) terminates all sessions and remote connections.
      5) If password-based authentication is used during remote maintenance, determine whether the agency changes the passwords following each remote maintenance service.

7. Timeliness of maintenance: Determine whether the agency:

A. Schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacture/vendor specifications and/or organizational requirements.
B. Maintains a maintenance log for the information system that includes:
   1) Date and time of maintenance.
   2) Name of the individual performing the maintenance.
   3) Name of escort, if necessary.
   4) A description of the maintenance performed.

8. Determine whether the agency has a continuity of operations process.

   A. Ensure that there is a continuity of operations plan and procedures for the agency's most critical means of communication.
   B. Confirm that the agency has tested the recovery of the E-mail system during a disaster recovery exercise.

Appendix P
Objectives for Evaluating Web Server Security

Overall Objective
The overall objective of this audit is to determine whether the agency has implemented effective security controls to protect its web servers and applications.[110]

Detailed Sub-Objectives

1. Determine the Internet Protocol (IP) addresses for all agency public-facing web servers through the use of Office of Inspector General scanning tools.

    A. Use the Nmap scanning tool to perform discovery on the agency's network environment.
    B. If necessary, perform a scan using Nmap to determine the system environment.
    C. Identify all public-facing web servers belonging to the respective domains known by Google.
    D. Analyze results to determine IP addresses, server name, locations, and hosts that belong to all agency public-facing web servers.

2. Evaluate whether the agency has implemented effective security controls to protect its web servers.

    A. Assess whether the web server operating systems have been updated and critical security patches have been applied.
    B. Ensure that unnecessary services have been disabled or removed from web server operating systems.
    C. Verify whether effective user authentication controls have been implemented on web server operating systems.
    D. Assess whether effective privileged account controls have been implemented on web server operating systems.
    E. Ensure that any additional security controls have been implemented to protect web server operating systems from unauthorized use.
    F. Verify that effective security monitoring, vulnerability testing, and audit log review are being performed on web server operating systems.

3. Evaluate whether the agency has implemented effective security controls to protect its websites and applications.

[110] References to "agency" apply to any responsible office, component, or governing body.

A. Ensure that website applications have been updated and critical security patches have been applied.
B. Assess whether unnecessary services have been disabled or removed from website applications.
C. Verify that effective user authentication controls have been implemented on website applications.
D. Ensure that effective privileged account controls have been implemented on website applications.
E. Assess whether effective security controls have been implemented on website application resources and data.
F. Verify that effective security monitoring, vulnerability testing, and audit log review are being performed on website applications.
G. Assess whether cross-site scripting and Structured Query Language injection vulnerabilities have been identified or mitigated on website applications.
H. Ensure that cookies are not being used by website applications.

4. Determine the IP addresses, Fully Qualified Domain Name (FQDN), location, and responsible personnel for all agency public-facing web servers.

   A. Obtain a list of IP addresses belonging to public-facing web servers.
   B. Request the FQDN for the servers.
   C. Determine which web servers belong to which application(s).
   D. Determine responsible personnel for each group of applications or each web server and obtain a point-of-contact.
   E. Query agency business owners to determine whether there are additional public-facing web servers in the environment that do not fall under the responsibility of Information Technology.

5. Using scan results, such as WebInspect, identify the following for web servers:

   A. Current patches are installed as required by policy.
   B. Passwords meet agency standards.
   C. Contain fields subject to injection flaws.
   D. Have authentication and session management vulnerabilities.
   E. Have insecure direct object reference.
   F. Use cross-site request forgery.
   G. Use of secure cryptographic storage.
   H. Failure to restrict Uniform Resource Locator access.
   I. Insufficient transport layer protection.
   J. Invalidated redirects and forwards.
   K. Use of cross-site scripting.

Appendix Q
Objectives for Evaluating DNS Server Security

Overall Objective
The overall objective of this audit is to determine whether management and security measures are in place over Domain Name System (DNS) servers within the agency.[111]

Detailed Sub-Objectives

1. Determine the location and ownership of DNS servers throughout the agency.

   A. Request a list of servers maintained by the agency as well as a list of all organizational elements that maintain their own servers.
   B. Identify a methodology to select specific DNS servers for audit testing.

2. Evaluate whether the agency has implemented Office of Management and Budget (OMB) Memorandum 08-23 DNS Security (DNSSEC) policies.

   A. Assess whether the DNSSEC Deployment Plan Outline contains:
      1) Enumerate .gov Domains – Enumerate the second-level domains beneath .gov operated by your agency (or on behalf of your agency). Only the second-level sub-domains need to be listed.
      2) Sources of DNS Services – For each domain, the Outline should describe whether the agency DNS administration and server operation are provided in-house, outsourced to a commercial provider (e.g., vendor), or delivered by other means (e.g., provided by another agency).
      3) DNS Server Infrastructure Description – Document the provider, vendor, or source of DNS server implementations within your agency (e.g., Berkeley Internet Name Domain, Name Server Daemon, and Microsoft Advanced Directory). Include in your estimate the number of such servers per source.
      4) Barriers – Document any perceived technical, contractual, or operational barriers impeding deployment of DNSSEC, and milestones for addressing each.
      5) Training – Review the activities of the U.S. Government Secure Naming Infrastructure Pilot at www.dnsops.gov and your agency's training workshops.
      6) Plan of Action and Milestones – Document your agency's Plan of Action and Milestones to implement the policies described in the OMB memorandum. In particular, this plan should detail all key activities (e.g., acquisition if necessary, training, testing, deployment, operations plans with priority given to citizen services and E-government domains, especially those that collect any personally identifiable

[111] References to "agency" apply to any responsible office, component, or governing body.

information) and milestones necessary to achieve the goal of fully operating DNSSEC signed .gov sub-domains.

B. Request the documentation provided to OMB to verify that it contains the above items.

2. Evaluate whether DNSSEC has been implemented at the agency.gov domain and sub-domains.

   A. Ensure that DNSSEC is deployed at second-level domains (i.e., agency.gov), as required by OMB.
   B. Ensure that all systems, low, medium, and high, are secured by implementing transmission integrity and secure name/address resolution controls, as required by the National Institute of Standards and Technology (NIST).
   C. Verify whether commercial software is used to determine whether servers have DNSSEC implemented.

3. Evaluate whether the DNS servers deployed within the agency adhere to the checklist provided in NIST Special Publication 800-81. Select a sample of checklist items that can be tested using commercial software to verify that the settings are compliant.

4. Evaluate whether DNS servers in the agency are free from vulnerabilities caused by misconfigurations or software flaws.

   A. Using the agency's vulnerability assessment and patch management solution (e.g., BigFix), verify that the server is compliant with NIST requirements.
   B. Obtain a list of all agency DNS servers and determine whether the assessment tool identifies each.

5. Evaluate whether the agency's DNS servers have been patched or updated as required by the agency as a result of a DNS incident.

   A. Ensure that all vulnerability and weaknesses identified have been reported to the DNS servers' administrators.
   B. Verify that the agency has taken corrective actions, conducted proper follow-up on all known incidents, and reported on the results.

Appendix R
Objectives for Evaluating Firewall Security

Overall Objective
The overall objective of this audit is to determine whether agency perimeter firewalls, routers, and switches are securely configured.[112]
(**Note:** The detailed sub-objectives are based on an evaluation of Cisco firewalls.)

Detailed Sub-Objectives

1. Review background information about the firewall(s), e.g., segment diagrams, software, hardware, routers, version levels, host names, Internet Protocol [IP] addresses, connections, any specific policies for an overview of the firewall security.

   A. Ensure that appropriate filtering exists.
   B. Ensure logging is enabled on the firewall. The minimum level should be set to 4.
   C. Enable logging as follows:
      1) Define log server – logging host [in_if_name] ip_address [protocol/port].
      2) Define type of messages to be logged – logging trap level.
      3) Issue logging on to start logging.
   D. Ensure that a syslog server is used to store logged messages.
   E. Ensure that logs are generated and stored securely on a separate partition or server.
   F. Analyze whether the firewall(s) has compilers, editors, or any other type of development tool.
   G. Run the show central processing unit (CPU) usage command to determine if it is overworked. It should not be running over 30 percent.
   H. Ensure that all firewalls have appropriate login banners.

2. Evaluate whether all firewall-related policies (administration, change control, logging, backup and recovery, etc.) are documented.

   A. Ensure that the stated polices (e.g., administration, change control, logging, backup and recovery) have been developed and implemented. These policies should explicitly address the periodic review of firewall security and the regular reviewing of audit logs. Review the policies for appropriateness.
   B. Use Simple Network Management Protocol (SNMP) to evaluate firewall monitoring procedures. This is achieved as follows:
      1) Set the IP address of the SNMP server – snmp-server host. Set the location, contact, and the community password snmp-server options.

[112] References to "agency" apply to any responsible office, component, or governing body.

2) Use logging trap to set logging level. Use the errors levels to define logging levels.
3) Logging on – command to start sending System Log (syslog) messages to the server. No logging on – to disable sending messages.
4) A risk of non-detection of system issues exists if the state of the firewall is not monitored.
5) Use show SNMP server to check configurations.

3. Review whether the default firewall ports are open. These ports are for administration and should disabled. Attempt to port scan the firewall(s), from both the internal network and the Internet, scanning for Internet Control Message Protocol (ICMP), User Datagram Protocol, and Transmission Control Protocol.

4. Assess whether a lockdown rule is included at the beginning of the rule base.

   A. Ensure that administrative access is granted before the lockdown rule is put into place. (**Note:** All other rules should go after the lockdown rule, going from most restrictive to general rules.)
   B. Review for number of connections. Increase/decrease the number of connections to 50,000. This makes it more difficult to fill the connections table.
   C. Attempt to test the rule base by scanning secured network segments from other network segments.
   D. Ensure that the firewall is enforcing organizational expectations and is accepting **only** the traffic that is authorized.
   E. Place a system on the demilitarized zone (DMZ) and attempt to penetrate the secured segments, as the DMZ is highly vulnerable.

5. Identify accessible resources behind the firewall that are to be encrypted and determine that these connections are encrypted.

6. Ensure the accuracy with the show clock command.

   A. Ensure that Network Time Protocol (NTP) is used to keep accurate time.
   B. Configure NTP to allow updates from the internal time servers only.
      1) Disable NTP on the Internet interface inbound and outbound.
      2) Synchronize your Internet Access time with the rest of your network.

7. Ensure that web-filtering software is used on the firewall.

8. Identify whether Hypertext Transfer Protocol inspection is enabled.

9. Verify that the following protocols run through the firewall; they should be disabled:

A. FTP – File Transfer Protocol.
B. NIS – Network Information Services.
C. NFS – Network File System.
D. UUCP – Unix-to-Unix Copy.
E. X – Windows System.
F. Finger.

10. Ensure that access lists have been applied to control the flow of network traffic.

    A. Analyze whether the firewall drops active code from incoming web traffic.
    B. Ensure that all access lists have been applied to the appropriate interfaces.
    C. Ensure that static and conduit statements have been applied to control the flow of network traffic.

11. Ensure that configuration files are stored as back-ups elsewhere and in secure locations.

12. Ensure that ICMP type 3 and 5 packets have been disabled.

13. Ensure that the firewall(s) is properly documented.

    A. Review network diagrams to ensure that all firewalls and network appliances have been documented.
    B. The following should be listed:
       1) Version number.
       2) Location.
       3) Host name.
       4) Internet connections.

14. Ensure that Network Address Translation is used to hide the IP addresses of the internal network from external networks.

15. Ensure that proxy-Address Resolution Protocols have been disabled.

16. Ensure that random, longer than 30 character, cryptic secret key is used for manual IP Security, where:

    A. Encryption keys are renewed on a timely manner.
    B. Crypto Access Lists are implemented.

17. Ensure that appropriate session timeout values have been assigned.

18. Ensure that SNMP is disabled or non-default community strings are required for SNMP access.

19. Ensure that an enabled password exists on all firewalls.

20. Review for dial in access directly to the firewall server.

21. Ensure that adequate physical security controls are in place to restrict access to firewall and Domain Name System servers.

22. Ensure that appropriate disaster recovery arrangements exist for the firewall to reduce downtime due to a firewall outage.

    A. Ensure that the firewall is covered in the agency's disaster recovery plans.
    B. Ensure that failover systems exist. Ensure that failover systems are the same as the main firewall to allow for successful failovers.
    C. Ensure that a universal power supply exists. Power outages or fluctuations could cause disruptions.

Appendix S
Objectives for AD Testing

Overall Objective
The overall objective of this audit is to determine whether the agency has designed and implemented Active Directory (AD) services to effectively manage access to its systems and services.[113]

Detailed Sub-Objectives

1. Evaluate whether the agency has implemented trust zones to ensure security and interoperability across domains.

   A. Verify that the agency maintains a list of all domains (within the forest).[114]
   B. Ensure that the agency maintains documentation of how trusts are configured between the agency and all its components. Document:
      1) Trust type (external, forest, or realm).
      2) Fully qualified domain names of each party.
      3) Direction (one-way or two-way).
   C. Ensure that trusts are configured as one-way whenever possible.
   D. Ensure that the trusted systems are secured according to agency policy.

2. Evaluate whether the agency has designed an enterprise AD solution to support agency goals.

   A. Ensure that the agency maintains accurate design documentation for AD.
   B. Assess whether the agency has developed adequate short and long-term plans for the following agency-wide programs and initiatives, as they relate to AD:
      1) Homeland Security Presidential Directive 12 logical access.
      2) Implementation of agency single sign-on identities for employees.
      3) U.S. Government Configuration Baseline.
      4) Domain Name Service (DNS) security.

3. Evaluate whether the agency has implemented effective account management and access controls on AD services.

[113] References to “agency” apply to any responsible office, component, or governing body.
[114] The AD framework that holds the objects can be viewed at a number of levels; the forest, tree, and domain are the logical divisions in an AD network. At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

A. Ensure that effective privileged account controls have been implemented for root administrators, domain administrators, enterprise administrators, DNS administrators, or any others with AD access.
B. Ensure that written procedures exist and followed to identify and disable inactive accounts in a timely manner.

4. Evaluate whether the agency's secure baseline configuration guide has been implemented for agency AD services.

Appendix T
Objectives for Evaluating Incident Response, Handling, and Reporting

Overall Objective
The overall objective of this audit is to determine whether the agency has an effective system for detecting, reporting, and responding to security incidents, in accordance with Federal regulations, and established standards and guidelines.[115]

Detailed Sub-Objectives

1. Evaluate whether the agency has implemented a process for its incident response capability.

   A. Assess whether the agency has taken steps to address lessons learned from previously detected incidents.
   B. Identify whether the agency performed a detailed review to identify and create a lessons learned document.
   C. Interview officials to determine the status of implementing corrective actions to address areas of concern identified.
   D. Ensure that incidents are being reported to the:
      1) Information Systems Security Officer.
      2) Computer Security Incident Response Center (or agency response team).
      3) Agency call center.
      4) Department of Homeland Security's U.S. Computer Emergency Readiness Team, as appropriate.
   E. Verify that the agency has tested corrective actions to address the areas of concern identified.
   F. Determine whether management has implemented controls to address issues identified and obtain evidence that shows the implemented controls address vulnerabilities.
   G. Identify any reasons why the agency has not taken actions to address the recommendations; document the reason(s) for any delays.
   H. Analyze whether internal policies and procedures have been updated to incorporate any newly implemented actions.
   I. Verify that an action plan has been developed or the reason(s) for any delays.
   J. Ensure that the agency has tested all corrective actions to verify that the implemented controls remediated the issue.

2. Evaluate the tool(s) the agency has implemented to increase its capability to promptly identify, analyze, and resolve cybersecurity incidents against the agency's network.

[115] References to "agency" apply to any responsible office, component, or governing body.

A. Request IT officials to provide the following information from each technical tool(s) that is used to help identify and analyze cyber-security incidents on the agency's network:
   1) The cost.
   2) Person responsible for rolling-out the tool(s).
   3) The project and implementation plan and status.
B. Assess whether there have been any delays in implementing the tool(s). If so, interview the management team responsible for implementing the tool to determine the reason(s) for any delays.
C. Identify whether the tool(s) will be centrally managed and who is responsible for managing and monitoring the tool.
D. Obtain a copy of the agency network diagram and determine whether it complies with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61.
E. Evaluate whether the placement of the tool(s) provides adequate coverage for monitoring the agency's network traffic.
F. Obtain a copy of the agency's audit logging policy and assess whether the policy complies with NIST SP 800-92.
G. Assess whether other log (event) management tool(s) are being used to capture/log network traffic.
   1) Identify the responsible personnel for the log management (event) tool(s).
   2) Review how the log management tool(s) is being used and where the tool(s) is located.
   3) Verify the type of auditable events the log management tool(s) is configured to capture.
   4) Identify any concerns or issues with the reliability, capability, or performance of the log (event) management tool(s).
   5) Review a sample of the tool(s) reports to confirm that the log (event) management tool(s) is capturing the designated auditable events.
   6) Assess whether the logging reports are complete or include unfragmented data based on the tool(s)' reporting features.
   7) Identify who is responsible for reviewing the log management reports and documentation.
   8) Determine how often the reports are reviewed.
   9) Examine where the reports are maintained and whether the location prohibits unauthorized access.
      a. Review how access to the reports is controlled.
      b. Identify whether controls are in place to restrict access to reports.
   10) Assess how long the reports are retained or stored and where the reports are archived.

H. Distribute an E-mail message to all Information Security Officers to identify whether any local technical tools were installed on the network to combat cybersecurity incidents. If technical tools were installed locally, identify the:
    1) Cost.
    2) Tool's purpose.
    3) Date the tool was installed.
    4) Location on the local network.
    5) Controls in place to limit access to the reports.
    6) Person responsible for reviewing the tool's reports.
    7) Authorization for installing the tool.
    8) Training or guidance on how to use the tool.
I. Identify whether any local security incidents have been detected using the technical tools. If security incidents were detected, identify:
    1) The individual who identified the security incident.
    2) The type of incident.
    3) When the security incident occurred.
    4) Where the incident occurred.
    5) How the incident was detected.
    6) The cause of the security incident.
    7) Whether corrective action(s) were implemented to secure the vulnerability that allowed the incident to occur.
    8) Whether controls were put in place and tested to ensure that similar incidents would not occur.
J. Ensure that the agency's headquarters was notified of the incident, corrective actions were implemented, and the newly implemented controls were tested. Obtain documentation.

Appendix U
Objectives for Evaluating IPv6

Overall Objective
The overall objective of this audit is to determine whether the agency is effectively managing its implementation of Internet Protocol, version 6 (IPv6).[116]

Detailed Sub-Objectives

1. Determine whether the agency is effectively planning for its transition from Internet Protocol, version 4 (IPv4) to IPv6.

   A. Ensure that the agency has established an IPv6 project office with clearly defined roles and responsibilities for IPv6 implementation.
      1) Ensure that the agency has assigned an official to lead and coordinate the agency's transition from IPv4 to IPv6.
      2) Evaluate whether the project office monitors and oversees the agency components' efforts to implement IPv6.
      3) Ensure that the components have assigned an official or established a project office to plan for the transition to IPv6.

   B. Determine whether the agency has developed an IPv6 transition plan as part of its Enterprise Architecture submission to Office of Management and Budget (OMB). The detailed transition plan should be applicable for all agencies and identify the following:
      1) Network infrastructure.
      2) Address schema.
      3) Network topology with routing protocol.
      4) Transition mechanisms selected for the conversion (i.e., dual-stack, tunnels).
      5) Training within the multiple disciplines required to transition to IPv6.
      6) Costs associated with implementing IPv6 on top of IPv4. (Costs will most likely come from software and hardware, training, application porting, consulting services, and operational costs.)
      7) A detailed transition schedule with interim milestones to migrate to IPv6.

   C. Ensure that a process has been established to monitor the agency and organizational components' progress in meeting these milestones.

   D. Identify whether the agency has issued any guidance for its implementation to IPv6. Evaluate whether the guidance is adequate.

   E. Identify whether OMB has reviewed the implementation plan and approved the agency's milestone dates.

[116] References to "agency" apply to any responsible office, component, or governing body.

2. Determine whether the agency has completed an inventory to assess the current level of IPv6 capability.

   A. Ensure that the agency and its components have accurate inventories of devices and applications that may be affected by the transition to IPv6.
      1) Ensure that the agency has conducted an initial agency-wide inventory of existing routers, switches, and hardware firewalls.
      2) Evaluate how the agency verified the accuracy of its initial inventory. Ensure that the inventory contains the manufacturer, model, and serial number of the devices.
      3) Ensure that the agency has conducted a comprehensive inventory to account for all existing applications and other devices, not captured in the initial inventory that may be affected by the transition to IPv6.
      4) Ensure that the agency has a process to verify that all new acquisitions for information technology (IT) devices and technology procurements that include a viable upgrade path are IPv6 compliant.
      5) Ensure that the agency has developed plans or a process for maintaining its IPv6 inventory.
      6) Identify whether components have established a process to ensure that products are not counterfeit.
         a. Ensure that IPv6 devices are registered with the manufacturers.
         b. Ensure that IPv6 equipment uses certificates between devices.
   B. Ensure that the agency has identified devices that are not, and never will be, IPv6 capable.
   C. Ensure that the agency has developed an impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6.
   D. Ensure that any newly acquired devices or technology are IPv6 compliant.

3. Determine whether the agency has effectively planned for and communicated the interim operability between IPv4 and IPv6.

   A. Ensure that the agency has documented its existing IPv4 network topology and its vision for its IPv6 network topology, to include:
      1) Number of external networks accessed from within the agency and means of access to service providers.
      2) Number of local area networks within the agency.
      3) Number of devices, nodes, and in general, number of networked entities assigned or to be assigned IPv6 addresses.
   B. Ensure that the agency has determined the IPv6 address space it will require over the next 5-year period and made its request for IPv6 address assignment for deployment from the American Registry for Internet Numbers.
   C. Evaluate what the agency components are doing regarding the IPv6 transition.

D. Ensure that milestones have been established to measure progress in implementing IPv6 at the agency headquarters and its components.
E. Ensure that the implementation strategy is considered for future IT investment decisions, including ensuring that IT investments appropriately address agency IPv6 requirements.
F. Ensure that the agency has communicated its IPv6 transition planning to all its components.
G. Ensure that training materials have been developed to inform stakeholders (e.g., administrators) about the transition.

4. Determine whether the agency is effectively planning for testing the integration of IPv6.

   A. Identify whether the agency and its components have developed a testing plan to evaluate its IPv6 capabilities. Ensure that the plan identifies the following:
      1) Availability and operability of testing facilities.
      2) Methods of testing.
      3) Transition mechanisms, security, conformance, and interoperability between IPv4 and IPv6 devices.
   B. Review test documentation, reports, and conclusions on IPv6 functionality and evaluate the quality of the tests.
   C. Identify the planning efforts being conducted to test devices and networks not yet tested for IPv6 capabilities.
   D. Evaluate whether selected network devices are configured properly and ensure the following:
      1) Selected IPv6 features, which are prohibited by the agency IT security policies, are disabled (e.g., peer-to-peer services).
      2) Addressing allocation strategies and scoping rules are used.
      3) Routers fully comply with NIST IPv6 specifications and are enabled with proper routing protocols.
      4) Transition and co-existence mechanisms are compatible for both IPv4 and IPv6.
      5) Router interfaces are enabled with IPv6 support Network Layer 2 link technologies.
      6) IP Security is implemented on all IPv6 stacks and enabled on network devices.
      7) Cryptographic operations, performed by IP Security and Internet Key Exchange, are aligned with Federal Information Processing Standard requirements.

Appendix V
Objectives for RFID Testing

Overall Objective
The overall objective of this audit is to determine whether the agency has effectively implemented Radio Frequency Identification (RFID) to protect its mission critical data.[117]

Detailed Sub-Objectives

1. Evaluate whether the agency has developed adequate policies and procedures to ensure the confidentiality, integrity, and availability of data contained on RFID tags, readers, and databases.

   A. Ensure that policies have been established for implementing RFID technology.
   B. Ensure that procedures have been established for each RFID device (tag, reader, and database).
   C. For RFID systems under development, ensure that security is included during the development process.

2. Evaluate whether security controls implemented on RFID devices are effective.

   A. Assess the following attributes for each tag:
      1) Identify the type of tag (passive, semi-passive, active), memory, and frequency used.
      2) Identify the data that is being stored on the tag.
      3) Ensure that adequate processes have been established for the:
         a. Distribution of tags.
         b. Physical security of tags not in use.
         c. Destruction of tags.
         d. Training of employees on installation and maintenance of tags.
      4) Ensure that adequate security is implemented on the tag and the transmission of data to/from the tag.
   B. Assess the following attributes for each reader:
      1) Identify the storage capacity, processing capacity, and frequency of readers.
      2) Ensure that adequate physical controls have been established to restrict access to the reader.
      3) Ensure that encryption is used to protect the data that is transmitted to and from the reader.
   C. Assess the following attributes for the database:
      1) Identify the type of database used.

[117] References to "agency" apply to any responsible office, component, or governing body.

2) Ensure that adequate physical controls have been established to restrict access to the database server(s).
3) Ensure that adequate security controls are implemented on the database and database servers containing RFID data (i.e., scan database and servers for vulnerabilities).
4) Identify and examine a current list of users and their authorized level of access to the database.
5) Identify the process for the administration of user identifications and passwords, and the level of access to the database.
6) Ensure that password settings are adequate and rules are based on agency password requirements.
7) Ensure that user access rules are defined and reviewed periodically to determine if they are still appropriate and updated as necessary (i.e., when privileges change).
8) Identify whether audit trails are recording who accessed and modified the database.
9) Identify whether audit trails are reviewed and maintained. Ensure that access controls over audit trail records are established and limited to system administrators and security administrators.
10) Ensure that backup, disaster recovery, and contingency planning is adequate. Test for the following:
    a) Contingency plan has been developed and tested periodically.
    b) Critical files are backed-up to removable media periodically and stored off-site.
    c) Arrangements are made for alternate data processing and telecommunication facilities.
    d) Event logs are generated when backup operation is performed.

3. Evaluate whether privacy issues have been addressed in the implementation of RFID.

   A. Ensure that a privacy impact assessment was performed in accordance with the E-Government Act of 2002.
   B. Ensure that individuals are notified about the use of RFID (e.g., signs posted, pamphlets, documents informing users).
   C. Identify how the agency is using the data collected from the tags (e.g., tracking, profiling).
      1) Ensure that a memorandum of agreement/understanding is established if the data collected is shared with other agencies.
      2) Ensure that individuals have the right to ask whether personal data was shared with other agencies and/or businesses.
      3) Assess whether an individual can request to have data deleted from the tag.

Appendix W
Objectives for Evaluating Insider Threats

Overall Objective
The overall objective of this audit is to determine how effectively the agency protects its information systems and data from the threat posed by employees, especially those with special or elevated access to unclassified information technology (IT) systems or information based on their job description or function.[118]

Detailed Sub-Objectives

1. Evaluate whether the agency has established an insider threat program office to address the risk agency-wide. Assess whether:

    A. The agency has established a program office, working group, or other entity responsible for addressing insider threat risks agency-wide.
    B. The agency has addressed the insider threat risk by establishing roles and responsibilities, and insider threat-specific policies, procedures, and guidance.
    C. Policies exist to minimize the potential risk from a malicious insider with regard to loss, destruction, or theft of data.
    D. The agency has implemented an annual insider threat security awareness program for all employees.
    E. Employees are given the training/knowledge to assist the organization in recognizing and addressing potential or actual insider threat risks or attacks.
    F. The agency includes a cross-discipline insider threat incident handling team or working group.
    G. There is a process for ensuring that employees are knowledgeable and kept up to date regarding insider threat policies.

2. Evaluate whether there is an enterprise risk management process that addresses insider threats.

    A. Identify whether an agency possesses an enterprise risk management plan. If so, obtain a copy of that plan and assess how or if insider threat risks are identified, assigned, and addressed across the enterprise.
    B. Ensure that a risk management process is implemented consistently and continually across the agency.
    C. Review agency components' processes for assigning risk to information systems that aligns with the latest National Institute of Standards and Technology guidance.

[118] References to "agency" apply to any responsible office, component, or governing body.

3. Evaluate whether the agency consistently communicates insider threat risk policies and procedures across the enterprise. Assess whether:

   A. Agency organizations work separately or together to identify, prioritize, and address the insider threat risk.
   B. Communication among all agency organizations is continual and consistent to help ensure that new threats, attack vectors, and countermeasures are effectively handled.
   C. The agency disseminates and communicates its risk management strategy.
   D. The agency includes recognizing and reporting potential indicators of insider threat as a part of its security awareness training.

4. Evaluate whether potential candidates for hire are screened for the insider threat risk and that the agency performs background checks before determining suitability of a potential employee.

5. Evaluate whether the agency has a consistent process for removing system and building access when an employee retires, resigns, terminates, transfers, or is put on a leave of absence. Assess whether:

   A. Human Resources, management, and the security office are notified upon termination of an individual.
   B. The agency retrieves its property and software immediately upon an employee's exit.
   C. All system access is terminated timely when an employee, contractors, or other trusted partners terminate employment.
   D. Other employees are notified timely when an employee exits.

6. Evaluate whether the agency has the ability to identify and report an employee's unusual behavior. Assess whether:

   A. Supervisors are trained to monitor and respond to behaviors of concern exhibited by employees.
   B. Management, Human Resources, and security personnel work together when resolving employee conduct issues.
   C. Reports of policy violations are systematically recorded so that management, Human Resources, and security personnel can reach a fair decision.
   D. An employee who notices suspicious behavior by another employee knows how to report this behavior.

7. Evaluate how effectively the user account management process prevents unauthorized access to critical IT systems. Assess whether:

A. The agency has a procedure or process to verify against unauthorized backdoor accounts. Verify that these accounts do not exist.
B. There are any shared accounts and whether the accounts should be removed.
C. There are any expired or dormant accounts and how long they have been inactive.
D. The highest level of permission(s) granted to the system administrator(s) of that system is necessary and whether these permissions were properly approved in a formal authorization process.
E. The number of privileged (i.e., administrator or elevated access) accounts is equal to the number of formal authorizations that have been granted.
F. The component verifies the instances of unauthorized changes to user accounts or user access controls (level of access) on information systems.

Appendix X
Contributors to This Guide

This guide was prepared by:

Barbara Bartuska, IT Audit Manager, Office of IT Audits, DHS OIG
Patrick Nadon, Operations Manager, Office of IT Audits, DHS OIG

The following OIGs provided audit plans/programs for consideration:

Department of Defense
Department of Education
Department of Health and Human Services
Department of Housing and Urban Development
Environmental Protection Administration
Social Security Administration
Tennessee Valley Authority
United States Department of Agriculture
United States Postal Service

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig."

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.