OFFICE OF INSPECTOR GENERAL

CISA Should Validate Priority Telecommunications Services Performance Data

Homeland Security

January 10, 2022

OIG-22-15

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

January 10, 2022

MEMORANDUM FOR: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2022.01.07 13:00:27 -05'00'

SUBJECT: *CISA Should Validate Priority Telecommunications Services Performance Data*

For your action is our final report, *CISA Should Validate Priority Telecommunications Service Performance Data*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving the quality of CISA's priority telecommunications services performance data. Your office concurred with the recommendation. Based on information provided in your response to the draft report, we consider this recommendation open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

cc: Nitin Natarajan, Deputy Director, CISA
Billy Brown, Jr, Executive Assistant Director, ECD

DHS OIG HIGHLIGHTS

CISA Should Validate Priority Telecommunications Services Performance Data

January 10, 2022

Why We Did This Review

Priority Telecommunications Services leverage the public telephone network to provide telecommunication for national security and emergency preparedness during times of call congestion. We conducted this review in response to a hotline complaint regarding connectivity and testing of DHS' telecommunications services. Our objective was to determine whether DHS effectively supported operable and interoperable emergency communications for Federal, state, local, tribal, and territorial government officials and critical infrastructure operators during the COVID-19 pandemic.

What We Recommend

We recommended that CISA establish a process to validate data reliability.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security, effectively ensured its Priority Telecommunications Services (PTS) program was operable early in the Coronavirus disease 2019 (COVID-19) pandemic. We conducted this review in response to an April 2020 Office of Inspector General hotline complaint about a failure in telecommunication connectivity and largely untested telecommunications services. We were able to confirm that:

1. the disconnection was an isolated event;
2. the telecommunications service provider developed a technical solution to prevent the problem from occurring again; and
3. CISA conducted periodic tests and coordinated simulated tests of priority telecommunications services.

We also determined that although CISA measures the performance of two of its priority telecommunications services, it does not have an adequate process in place to validate its performance data. As a result, CISA could report inaccurate information or misrepresent the effectiveness of its PTS program in its quarterly report to the DHS Chief Financial Officer.

CISA Response

CISA concurred with the recommendation.

Background

During emergencies, the public telephone network is critical for emergency responders and Federal, state, local, tribal, and territorial (FSLTT) government officials to maintain communications. However, commercial networks can become congested due to high call volumes, hindering the ability of first responders, national security and emergency preparedness, and response personnel to complete calls. Depending on the event severity (i.e., natural disaster, evacuation, heavier than normal peak period calling), network overloads can last for hours or even days. It is essential that communication services are operable during an emergency or crisis when the network is congested, such as during Coronavirus disease 2019 (COVID-19) pandemic response efforts.

In addition to ensuring operability, public safety communications preparedness requires fostering and maintaining high levels of interoperability in all types of response communications. For example, first responders and local emergency management agencies use a diverse range of communications to maintain situational awareness in heavily populated events and to communicate when radio channels and commercial wireless lines are in heavy use. Such diverse communications must be interoperable.

According to Executive Order 13618[1] (EO 13618) and Presidential Policy Directive 40,[2] the Department of Homeland Security, in conjunction with other Federal agencies, is required to oversee the development, testing, implementation, and sustainment of national security and emergency preparedness communications, including communications that support continuity of government, as well as FSLTT governments' emergency preparedness and response communications. DHS, along with other Federal agencies, is also required to ensure interoperability, availability, and restorability of those communications. After passage of the *Homeland Security Act of 2002*,[3] the Cybersecurity and Infrastructure Security Agency (CISA) became responsible for coordinating emergency communications and collaborating with Federal agencies and state and local governments, as well as telecommunications service providers, on emergency communications. CISA's mission is to partner with industry and FSLTT governments to understand and manage the risk to our Nation's critical infrastructure, including telecommunications. CISA is also responsible for developing guidance on emergency communications grant programs; establishing criteria for statewide

[1] *Assignment of National Security and Emergency Preparedness Communications Functions*, Executive Order 13618, July 6, 2012.
[2] *National Continuity Policy,* Presidential Policy Directive 40, July 15, 2016.
[3] *Homeland Security Act of 2002*, Public Law 107-296, November 25, 2002.

communications interoperability plans; and developing strategies and recommendations for the use of emergency communication technologies.

CISA Emergency Communications Program

EO 13618 authorized the Emergency Communications Division, within CISA, to establish programs for national security and emergency preparedness. The Emergency Communications Division provides guidance for assessing the communications capabilities of FSLTT governments' public safety agencies. This division is also the program manager for the Priority Telecommunications Services (PTS) program, a national security and emergency preparedness telecommunications program that leverages the public telephone network to provide priority telecommunications for national security and emergency preparedness. PTS is used during natural disasters, terrorist acts, and special events and consists of five distinct communications services:

1. Government Emergency Telecommunications Service (GETS) – provides priority local and long distance calling when landline networks are congested.
2. Wireless Priority Service (WPS) – provides priority calling when cellular networks are congested.
3. Telecommunications Service Priority – provides priority installation and repair of critical data and voice communications circuits.
4. Special Routing Assistance Service (SRAS) – provides enhanced routing and priority call capabilities implemented by GETS and WPS that is not traceable.[4] SRAS operates on three levels:
    - SRAS Level 0 is the default state where users must enter their GETS Personal Identification Number to make priority calls.
    - SRAS Level 1 is generally activated during emergency situations, exercises, and testing.
    - SRAS Level 2 requires activation for use during extreme emergency situations.[5]
5. Next Generation Network Priority Service – provides priority voice, data, and video communications.

These five services help emergency responders and FSLTT government officials who rely on a mix of devices to communicate during critical moments via cellular, landline, private network, and satellite. For example, WPS is used at sporting events, such as football games, to ensure that crucial calls go through. In addition, authorized FSLTT government officials and public safety personnel use WPS to gain priority access on wireless networks and ensure crucial

[4] This service deals with classified communications.
[5] According to CISA officials, SRAS Level 2 has never been activated.

communication during natural disasters and potential threats, such as terrorist events and criminal activities.

In 2019, CISA put forth a strategy, known as the *National Emergency Communications Plan,* to strengthen and enhance these emergency communications capabilities. This plan establishes a shared vision for emergency communications and assists stakeholders in response and recovery operations. The plan includes six goals covering Governance and Leadership; Planning and Procedures; Training, Exercises, and Evaluation; Communications Coordination; Technology and Infrastructure; and Cybersecurity. As stated in the Planning and Procedures goal, CISA should incorporate risk management strategies to protect against and mitigate disruptions to mission-critical communications.

On March 11, 2020, the World Health Organization declared COVID-19 an international pandemic.[6] On March 13, 2020, the President proclaimed that the COVID-19 outbreak in the United States constituted a national emergency.[7] The first several weeks, between March and May 2020, were a critical timeframe for emergency communications and coordination between FSLTT government officials and critical infrastructure operators, such as those in telecommunications, emergency services, government facilities, and public health and health care. During this time, White House and DHS officials met to execute a Whole-of-America response to fight the COVID-19 pandemic and protect the public. Additionally, CISA published best practice guidance[8] for FSLTT governments establishing communications capabilities for alternate care sites during a health crisis or other disaster. The guidance describes the services the Telecommunications Service Priority and PTS can provide to alternate care sites to ensure they receive priority treatment for vital voice and data calls.

The objective of this review was to determine whether DHS effectively supported operable and interoperable emergency communications for FSLTT government officials and critical infrastructure operators during the COVID-19 pandemic.

[6] World Health Organization, March 11, 2020.
[7] *Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak*, Proclamation Number 9994, March 13, 2020.
[8] *Emergency Communications Best Practices for Establishing Alternate Care Sites,* September 24, 2020.

Results of Review

CISA Had Adequate Mechanisms to Ensure Its PTS Program Was Operable Early in the COVID-19 Pandemic

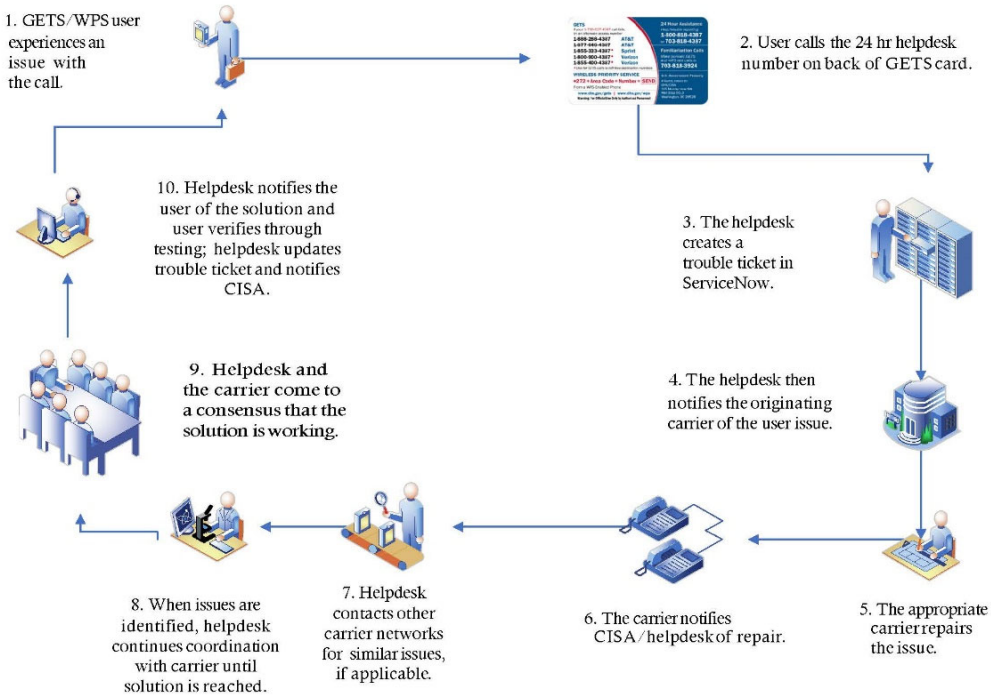
Through our review in response to an OIG hotline complaint, we determined CISA had adequate mechanisms to ensure its PTS program was operable early in the COVID-19 pandemic. OIG received a hotline complaint in April 2020 alleging there was a critical failure in telecommunication connectivity early in the COVID-19 pandemic. The complainant alleged that telecommunications services were largely untested and that critical failures were interrupting emergency response operations. The complainant also alleged that SRAS, which provides enhanced routing and priority call capabilities, was not being tested. Through our review, we were able to confirm that the disconnection was an isolated event, the telecommunications service provider developed a technical solution to prevent the problem from occurring again, and CISA conducted monthly stress tests and coordinated simulated tests of the PTS.

CISA investigated a disconnected call and discovered that, on April 17, 2020, calls made to a conference call line dropped 15 minutes after connection. After discovering the problem, CISA personnel worked with their GETS and WPS telecommunications helpdesk contractor, General Dynamics Information Technology (GDIT). Subsequently, GDIT notified the telecommunications service provider of the problem. According to the service provider's engineers, a "race condition"[9] caused calls to the conference call line to drop on April 17, 2020. This caused the interruption in service, as the system must process information in the proper sequence for the communication action to be processed. According to the service provider's engineers, this race condition was a unique case that had not been seen before. The engineers, while coordinating with CISA and GDIT, resolved the issue with a programming code change. On April 30, 2020, GDIT notified the user who initiated the trouble ticket of the technical solution and confirmed the problem was no longer occurring.

We also confirmed that CISA consistently works with the contractor to ensure GDIT supports PTS operational functions and resolves users' communication issues via a helpdesk ticket process, as shown in Figure 1.

[9] A race condition is when a system attempts to perform two or more operations simultaneously.

Figure 1. Processing Trouble Tickets



Source: DHS OIG-developed based on analysis of CISA-provided information

To ensure adequate call completion and quality, CISA examines automated national and international calls regularly. For example, in January 2021, CISA tested approximately 81,000 calls within the continental United States and tested approximately 4,000 calls outside the continental United States.

In response to the allegation that SRAS was not being tested, we confirmed that CISA personnel and GDIT performed routine tests to ensure GETS and WPS networks' operability during congestion. As stated previously, SRAS provides enhanced routing and priority call capabilities implemented by GETS and WPS. Specifically, GDIT, along with the telecommunications service providers, conducted periodic testing to ensure services were functioning according to requirements. We confirmed that GDIT conducted monthly Network Service Verification Tests from February through June 2020 to test for call completion, interoperability, and availability of services on SRAS Level 1 (used for emergency situations). In that time period, CISA personnel received a report each month from GDIT and telecommunications service providers that contained the results of all testing and issues. In addition, CISA conducted testing by initiating automated calls for Remote Services Verification Process

Tests[10] and International Inbound Test Procedures.[11]

However, according to CISA officials, the Department does not conduct live activation[12] of SRAS Level 2, which is activated for use during extreme emergency situations, because it is not cost effective. According to CISA, the cost of performing live activation is more than $2.5 million for the first 24 hours. Although DHS does not conduct live activation, we confirmed that CISA coordinated with a telecommunications service provider to conduct simulated testing[13] of SRAS Level 2 in 2019. The service provider conducted testing of the full SRAS control plans in April and October 2020 and conducted testing of a subset of the SRAS control plans in May and June 2020 to ensure functionality and effectiveness of the system.

CISA Measures Performance of Two Services under PTS but Does Not Have an Adequate Process to Validate Telecommunications Service Providers' Data

The *Government Performance and Results Act* (*GPRA) Modernization Act of 2010*[14] (the Act) requires quarterly performance assessments of Government programs to assess agency performance and improvement. In addition, the Act requires Federal agencies to ensure the accuracy and reliability of data used to measure progress toward performance goals, including identification of:

- means used to verify and validate measured data;
- sources for the data; and
- level of accuracy required for the intended use of the data.

We confirmed that, in compliance with the Act, CISA measures the performance of two PTS services, GETS and WPS, on a quarterly basis. The key performance parameter for each service is the call completion rate, which is the ratio comparing calls completed to calls attempted. CISA compiles these performance measures on a monthly basis using the following process:

[10] A Remote Services Verification Process Test allows telecommunications service providers to mimic the experience of a PTS user to determine whether GETS is working properly.
[11] International Inbound Test Procedures ensure successful call connectivity from an international location to a GETS platform.
[12] Live activation occurs when all telecommunications service providers operate in a bypass mode to provide users with simplified, uniform dialing procedures. Such activation occurs at the highest level of classified priority services.
[13] Simulated testing is an evaluation tool that validates the operability of a system or system components in a representation of the operational environment and in compliance with specified requirements.
[14] *GPRA Modernization Act of 2010*, Public Law 111-352, January 4, 2011.

- A CISA official receives telecommunications service providers' data on a monthly basis for GETS and WPS. This data includes total calls attempted, completed calls, incomplete calls, and blocked calls.
- The CISA official consolidates the telecommunications service providers' monthly data into the call completion rate.
- CISA combines the monthly call completion rates on a quarterly basis to obtain the quarterly performance measure.
- The CISA official forwards the quarterly performance measure to the Performance, Analysis and Evaluations Division within CISA.
- CISA provides this performance measure to the DHS Chief Financial Officer Performance Management Division, which in turn sends it to the Office of Management and Budget. The performance measure is ultimately reported to Congress in the Agency Financial Report.[15]

We reviewed fiscal years 2019 and 2020 GETS and WPS performance data to determine the reliability and accuracy of the reported information. During these two fiscal years, the targeted call completion rate was 99 percent for GETS and 85 percent for WPS. Specifically, in the second quarter of FY 2019, CISA reported GETS actual total calls made were 169,819, of which 168,425 (99 percent) were completed calls. In the third quarter of FY 2020, CISA reported GETS actual total calls made were 163,440, of which 163,104 (99 percent) were completed calls. The WPS actual call completion rate for FY 2019 was 97 percent and FY 2020 was 98.7 percent. We were provided the telecommunications service provider's raw data that made up the totals just mentioned. However, we were not able to recompute the quarterly performance measures from the telecommunications service providers' raw data.

Although CISA measures the performance of GETS and WPS, it does not have a formal quality control process in place to validate the data obtained and provided by the telecommunications services providers. CISA stated it had not yet established a consistent process for consolidating the monthly data because this was not identified as a necessary step to take when compiling performance reports. According to CISA, this was because although each telecommunications service provider submits its data in a different format, a quality control process is not necessary because telecommunications service providers' data is considered to be reliable under the terms and conditions of their contracts. Upon review, we determined that the contracts did not contain a clause requiring the providers to conduct data reliability verification and validation. Without a consistent process for compiling service provider data, we were not able to validate the data that was used to report these quarterly performance outcomes.

[15] U.S. Department of Homeland Security, FY 2020 Agency Financial Report.

As a result, CISA could report inaccurate information or misrepresent the effectiveness of its PTS program in its quarterly report to the DHS Chief Financial Officer. Until CISA establishes a process to validate the reliability of telecommunications service providers' data, it cannot be assured performance data is accurate or complete.

Recommendation

We recommend the Executive Assistant Director, Emergency Communications Division, establish a quality control process to validate the reliability of telecommunications service providers' performance data prior to consolidating *GPRA Modernization Act of 2010* Government Emergency Telecommunications Service and Wireless Priority Service performance measures for reporting to DHS.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from CISA. In its comments, CISA officials stated they appreciated the OIG's work to plan, conduct its review, and issue this report.

We reviewed CISA's comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. A summary of the Department's responses and our analysis follows.

CISA Comments to Recommendation 1: Concur. CISA's Emergency Communications Division officials agree there is a need to strengthen existing documentation and communications related to the quality control process for data validation. According to officials, the Division is in the process of ensuring all steps of the quality control process are well understood throughout the PTS Program. In addition, the Emergency Communications Division is committed to automating the process to reduce the administrative burden and increase accuracy on those executing the validation steps. However, Division officials do not believe additional testing or data validation is necessary. Officials believe it is best to strengthen existing processes, which is more cost effective.

CISA also noted that modernizing the process will not occur overnight. A plan is being developed to document requirements and identify what application(s) and process enhancements can streamlined. This effort entails a holistic review of how PTS Program data is transmitted, received, processed, stored,

and reported. While this effort has already begun, a concurrent effort focused on educating the appropriate personnel on the current data validation and quality control process is ongoing. Estimated Completion Date: May 31, 2022.

OIG Analysis of CISA Comments

CISA's actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

The objective of this review was to determine whether DHS effectively supported operable and interoperable emergency communications for Federal, state, local, tribal, and territorial government officials and critical infrastructure operators during the COVID-19 pandemic.

To gain an understanding of the telecommunications requirements, we reviewed the *Communications Act of 1934*, *Telecommunications Act of 1996, National Emergencies Act*, and the *National Security and Emergency Preparedness Communications Functions*, Executive Order 13618. In addition, we reviewed CISA's *Service Vendor Handbook for Telecommunications Service Priority Program* to understand the requirements for service vendors to comply with Telecommunications Service Priority program requirements. We also reviewed fact sheets for GETS and WPS eligibility. Further, we reviewed the processes for testing GETS and WPS using the Remote Services Verification Process System.

We interviewed multiple CISA officials and personnel to gain an understanding of its current procedures and processes. We also interviewed CISA contractual support personnel regarding the trouble tickets process. Further, we interviewed two selected telecommunications service carriers to discuss their processes for providing, maintaining, and troubleshooting telecommunications services. Lastly, we received a demonstration of the GETS and WPS Information Distribution System and Telecommunications Service Priority Web.

We compared CISA's FYs 2019 and 2020 GPRA Performance Measure Results data to determine the reliability and accuracy of the reported information.

We conducted this review between August 2020 and May 2021 pursuant to the *Inspector General Act of 1978, as amended*, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our review objective.

The Office of Audits major contributors to this report are Tarsha Cary, Director, Information Systems and Controls; Charles Twitty, Supervisory IT Auditor; Robert Williams, Program Analyst; Sonya Davis, IT Auditor; Donna Zavesky, IT Auditor; Kevin Dolloson, Communications Analyst; and Kate Fishler-Korotkova, Independent Referencer.

Appendix A
Management Comments to the Draft Report

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

December 8, 2021

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "CISA Should Validate Priority Telecommunications Services Performance Data" (Project No. 20-057-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Department is pleased to note OIG's recognition of the efforts undertaken by CISA's Emergency Communications Division (ECD), Priority Telecommunications Services (PTS) Program, to develop a technical solution to prevent future disconnection of priority calls, as well as testing that validates performance of priority services. CISA/ECD remains committed to ensuring an appropriately documented process is in place and communicated to the relevant stakeholders to further validate performance data of the priority telecommunications services.

The PTS Program is dedicated to making the test and evaluation of priority services as robust as possible to ensure it provides adequate data for Government Performance and Results Act reporting, while also maintaining good stewardship of taxpayer dollars. Accordingly, CISA/ECD currently conducts multiple Live Network Congestion Tests per year to verify the services meet established key performance parameters in a real-world congested environment. Moreover, a well-defined Systems Engineering Life Cycle process is in place, and CISA/ECD conducts Network Service Acceptance Tests with each Service Provider to validate the services work as designed during the development process. Post implementation, CISA/ECD conducts Network Service Verification Tests to verify the services continue to work in the field as designed. Also, throughout fiscal year 2021, the PTS Program upgraded 310 Wireless Priority Services devices to conduct testing using an enhanced Remote Service Verification Process, and more than 1,600 Remote Call Forwarding lines throughout the United States, which allow CISA/ECD to validate call completion, interoperability, and availability, as well as compare data that is collected independently with data that is provided by the Service Providers. Finally, CISA/ECD employs an Independent Test Agent that oversees testing from an unbiased and unburdened standpoint, which enables the PTS Program to identify any inconsistencies in the processes it uses to validate the reliability of the services it provides to the National Security/Emergency Preparedness community. In addition, this Test Agent provides ECD

confidence in the data it receives from the Service Providers, as there have not been any unexplained inconsistencies between data collected directly by the PTS Program and data transmitted to the Program by the Service Providers.

The draft report contained one recommendation with which CISA concurs. Attached find our detailed response to the recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in 20-057-AUD-DHS

OIG recommended that CISA's Executive Assistant Director of the Emergency Communications Division:

Recommendation 1: Establish a quality control process to validate the reliability of telecommunications service providers' performance data prior to consolidating GPRA Modernization Act of 2010 Government Emergency Telecommunications Service and Wireless Priority Service performance measures for reporting to DHS [the U.S. Department of Homeland Security].

Response: Concur. CISA/ECD agrees that there is a need to strengthen existing documentation and communications related to the quality control process for data validation. CISA/ECD is in the process of ensuring all steps of the quality control process are well understood by multiple personnel within the PTS Program. In addition, ECD is committed to automating the process to reduce the administrative burden and increase accuracy on those executing the validation steps. However, CISA/ECD does not believe additional testing or data validation is necessary. CISA/ECD believes it is best to strengthen existing processes which is more cost effective.

It is also important to note that modernizing the process will not be an overnight task. A plan is being developed to document requirements and identify what application(s) and process enhancements can streamlined. This effort entails a holistic review of how PTS Program data is transmitted, received, processed, stored, and reported. While this effort has already begun, a concurrent effort focused on educating the appropriate personnel on the current data validation and quality control process is ongoing. Estimated Completion Date: May 31, 2022.

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Executive Assistant Director, Emergency Communications Division, CISA
CISA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

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 Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305