~~FOR OFFICIAL USE ONLY~~

OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2019 (REDACTED)

~~WARNING: This document is For Official Use Only FOUO). Do not distribute or copy this report without the expressed written consent of the Office of Inspector General.~~

Homeland Security

~~FOR OFFICIAL USE ONLY~~

September 30, 2020

OIG-20-77

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 30, 2020

MEMORANDUM FOR: Randolph D. Alles
Senior Official Performing the Duties of the
Under Secretary for Management

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

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2019 – ~~For Official Use Only~~*

Attached is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2019 ~~– For Official Use Only.~~* We incorporated the formal comments provided by the Departmental GAO-OIG Liaison Office.

The report contains five recommendations aimed at improving the Department's Cybersecurity Workforce. The Department concurred with all five recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations 1, 2, 4, and 5 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Based on information provided in the Department's response to the draft report, we consider recommendation 3 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 and of the disposition of any monetary amounts. 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 final report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Information Technology, at (202) 981-6000.

cc: Chief Information Officer, DHS
Director, Cybersecurity and Infrastructure Security Agency (CISA)
Chief Information Officer, CISA

DHS OIG Highlights

Evaluation of DHS' Information Security Program for Fiscal Year 2019

September 30, 2020

Why We Did This Evaluation

We reviewed DHS' information security program for compliance with *Federal Information Security Modernization Act* requirements. We conducted our evaluation according to fiscal year 2019 reporting instructions. Our objective was to determine whether DHS' information security program and practices adequately and effectively protected data and information systems supporting DHS' operations and assets for FY 2019.

What We Recommend

We are making five recommendations to DHS to address the deficiencies we identified.

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

DHS' information security program was not effective for FY 2019 because the Department earned a maturity rating of "Ad Hoc" (Level 1) in three of five functions, compared to last year's higher overall rating of "Managed and Measurable" (Level 4). We rated DHS' information security program according to five functions outlined in the 2019 reporting instructions:

Identify — DHS received a Level 1 rating because it did not have an effective strategy or department-wide approach to manage risks for all of its systems.
Protect — DHS achieved Level 4 as it was rated Level 4 in three of the four domains essential to this function.
Detect — DHS received a Level 1 rating due to the lack of a comprehensive strategy and organization-wide continuous monitoring approach to address all requirements and activities at each organizational tier.
Respond — DHS received a Level 1 rating because the Coast Guard had not reported its cybersecurity incidents to DHS since 2012.
Recover — DHS received Level 3 because it had not made progress since prior years [redacted]

We attributed DHS' regress in managing its information security program to its recent decision [redacted] This decision adversely affected the Department senior leadership's ability to make informed and risk-based decisions on essential cybersecurity activities such as risk management, weakness remediation, system inventory, incident reporting, and continuous monitoring.

Management Response

DHS concurred with all five recommendations. We have included a copy of DHS' comments in Appendix B.

Table of Contents

Appendixes

Abbreviations

ATO	Authority to Operate
CBP	Customs and Border Protection
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Coast Guard	United States Coast Guard
DISA	Defense Information Systems Agency
[redacted]	[redacted]
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act

FLETC	Federal Law Enforcement Training Center
ICE	Immigration and Customs Enforcement
ISCM	Information Security Continuous Monitoring
IT	information technology
NIST	National Institute of Standards and Technology
NSS	National Security Systems
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personal Identifiable Information
POA&M	Plan of Action and Milestones
S&T	Science and Technology
Secret Service	United States Secret Service
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Services

Background

Recognizing the importance of information security to the economic and national security interests of the United States, Congress enacted the *Federal Information Security Modernization Act of 2014* (FISMA).[1] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. FISMA provides a framework for ensuring effective security controls over the information resources that support Federal operations and assets.

FISMA focuses on program management, implementation, and evaluation of the security of unclassified and national security systems (NSS). Specifically, FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs. Each program should protect the data and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. According to FISMA, agencies are responsible for conducting annual evaluations of information programs and systems under their purview, as well as assessing related information security policies and procedures. Each agency's Chief Information Officer (CIO), in coordination with senior agency officials, is required to report annually to the agency head on the effectiveness of the agency's information security program, including progress on remedial actions. The Office of the Inspector General (OIG) is responsible for conducting annual evaluations of information programs and systems under its purview, as well as assessing related security policies and procedures.

The Department of Homeland Security has various missions, such as preventing terrorism, ensuring disaster resilience, managing U.S. borders, administering immigration laws, and securing cyberspace. To accomplish its broad and complex missions, DHS employs approximately 240,000 personnel, all of whom rely on information technology to perform their duties. As such, it is critical that DHS provide a high level of cybersecurity for the information and information systems supporting day-to-day operations.[2]

The DHS Chief Information Security Officer (CISO) bears the primary responsibility for the protection of information and ensuring compliance with FISMA. Specifically, the DHS CISO heads the Information Security Office and manages the Department's information security program for its unclassified systems, its national security systems classified as "Secret" and "Top Secret," and systems operated by contractors on behalf of DHS. The CISO maintains

[1] Public Law 113-283 (December 18, 2014).
[2] Cybersecurity is the protection of internet-connected systems, including hardware, software, and data, from cyberattacks.

ongoing awareness of the Department's information security program, vulnerabilities, and potential threats through the execution of three programs: (1) Information Security Continuous Monitoring (ISCM) Data Feeds, (2) Ongoing Authorization Program, and (3) Security Operations Center. These programs provide a framework to govern the information systems owned and operated across DHS.

Foremost to all DHS components is adhering to requirements set forth in the DHS Security Authorization process, which involves comprehensive testing and evaluation of security features of an information system before it becomes operational within the Department. Per DHS guidelines, each component CISO is required to assess the effectiveness of controls implemented on all component information systems as part of the security authorization process, and periodically thereafter. The DHS CISO relies on two enterprise management systems to help administer its information security program and keep track of security authorization status. The enterprise management systems also provide a means to monitor plans of action for remediating information security weaknesses related to unclassified and Secret-level systems.[3]

FISMA Reporting Instructions

FISMA requires each agency Inspector General to perform an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. Further, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* provide OIGs with reporting requirements for addressing key areas identified during their independent evaluations of agency information security programs.[4] Each agency Inspector General has discretion to determine both an overall effectiveness rating as well as a rating for each of the Cybersecurity Framework functions (e.g., Identify, Protect, Detect, Respond, and Recover) at the maturity level of their choosing. Using this approach, the Inspector General may determine that a particular function area and/or the agency's information security program is effective at a maturity level lower than Level 4. IGs are required to assess the effectiveness of information security

[3] The National Institute of Standards and Technology (NIST) defines a security authorization as a management decision by a senior organizational official authorizing operation of an information system and explicitly accepting the risk to agency operations and assets, individuals, other organizations, and the Nation based on implementation of an agreed-upon set of security controls.
[4] The *FY 2019 Inspector General FISMA Reporting Metrics* were developed as a collaborative effort among the Office of Management and Budget (OMB), DHS, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council.

programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Within the maturity model context, agencies should perform risk assessments and identify the optimal maturity levels that achieve cost-effective security based on their missions and risks faced, risk appetites, and risk tolerance levels.

This report summarizes the results of our evaluation of the Department's information security program based on the FY 2019 FISMA reporting metrics, Version 1.3, dated April 9, 2019. The metrics align five functions from the NIST Cybersecurity Framework with eight domains established in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics.*[5] The NIST framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as shown in Table 1.

Table 1. NIST Cybersecurity Functions and FISMA Domains

Cybersecurity Functions		FISMA Domains
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	**Risk Management**
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services.	**Configuration Management**
		Identity and Access Management
		Data Protection and Privacy
		Security Training
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	**Information Security Continuous Monitoring**
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	**Contingency Planning**

Source: NIST Cybersecurity Framework and *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*

[5] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

According to the FY 2019 reporting instructions, OIGs are well positioned to assess agency information security programs, given their audit responsibilities and awareness of each agency's unique mission, cybersecurity challenges, and resources to address those challenges. Each OIG evaluates its agency's information security program using a set of questions cited in the reporting instructions for the five cybersecurity functions previously listed in Table 1. The questions are derived from the maturity models outlined within the NIST Cybersecurity Framework. Based on its evaluation, OIG assigns each of the agency's cybersecurity functions with a maturity level of 1 through 5. Table 2 describes each maturity level.

Table 2. IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1 – Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 – Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3 – Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 – Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5 – Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*

Per the FY 2019 FISMA reporting metrics, when an information security program is rated at "Level 4, Managed and Measurable," the program is operating at an effective level of security.[6] Agencies should perform risk assessments on an ongoing basis (either as part of security authorization or continuous monitoring processes) to identify their information system maturity levels based on cost-effectiveness, mission, and risk tolerance. Further, each OIG should apply a rating across the eight domains based on a simple majority. OIGs are encouraged to use the domain ratings to inform overall function ratings, and to use the five function ratings to inform the overall agency rating, based on a simple majority.

[6] *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.3, April 9, 2019.

Scope of Our FISMA Evaluation

We conducted an independent evaluation of the DHS information security program and practices based on the maturity model approach outlined in the FY 2019 Inspector General FISMA reporting metrics and NIST's Cybersecurity Framework. We performed our fieldwork at the DHS Office of the CISO and at selected DHS components.[7] To determine whether DHS components effectively manage and secure their information systems, we reviewed the Department's monthly FISMA Scorecards for unclassified systems and NSS.[8] DHS defines NSS as systems that collect, generate process, store, display, transmit, or receive Unclassified, Confidential, Secret, and Top Secret information.

As part of our review, we performed testing on three selected systems at United States Coast Guard (Coast Guard), Federal Emergency Management Agency (FEMA), and United States Citizenship and Immigration Services (USCIS) for compliance with applicable Defense Information Systems Agency (DISA) Security Technical Implementation Guides[9] settings on selected Windows 10 workstations, as well as the effectiveness of controls implemented on selected databases and servers. We responded to the questions cited in the FY 2019 reporting guidance based on our evaluation of DHS' compliance with applicable FISMA requirements and on our fieldwork performed at the DHS Office of the CISO, testing at Coast Guard, FEMA, and USCIS, and review of monthly FISMA Scorecards for unclassified systems and NSS.

To determine the effectiveness of components' implementation of their information security programs, our independent contractor performed work at CBP, CISA, and ICE to evaluate the components' procedures for identifying and managing cybersecurity risks based on applicable OMB and NIST guidance and the maturity approach outlined in the FY 2019 FISMA reporting metrics. Due to a delay in the contractor's onboarding process, we were unable to incorporate the contractor's results as part of our FY 2019 submission to OMB. However, we have incorporated the contractor's work into this report.

[7] U.S. Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), and United States Coast Guard (Coast Guard).
[8] The 2019 FISMA scorecard includes all DHS components we selected for review, as well as the Federal Law Enforcement Training Center (FLETC).
[9] The Defense Information Systems Agency issues Security Technical Implementation Guides for government agencies to implement for their computer systems to "harden" security settings.

Results of Evaluation

DHS' information security program was not effective for FY 2019 because the Department earned a maturity rating of "Ad Hoc" (Level 1) in three of five functions, compared to last year's higher overall rating of "Managed and Measurable" (Level 4). We rated DHS' information security program according to five functions outlined in the 2019 reporting instructions:

Identify — DHS received a Level 1 rating because it did not have an effective strategy or department-wide approach to manage risks for all of its systems.
Protect — DHS achieved Level 4 as it was rated at Level 4 in three of the four domains essential to this function.
Detect — DHS received a Level 1 rating due to the lack of a comprehensive strategy and organization-wide continuous monitoring approach to address all requirements and activities at each organizational tier.
Respond — DHS received a Level 1 rating because the Coast Guard had not reported its cybersecurity incidents to DHS since 2012.
Recover — DHS received Level 3 because it had not made progress since prior years [redacted]

We attributed DHS' regress in managing its information security program to its recent decision [redacted] This decision adversely affected DHS senior leadership's ability to make informed and risk-based decisions on essential cybersecurity activities such as risk management, weakness remediation, system inventory, incident reporting, and continuous monitoring.

DHS Must Strengthen the Management of Its Information Security Program

DHS' overall information security program is not effective because the Department achieved Level 1 in Identify, Detect, and Respond — three of the five cybersecurity functions listed in this year's FISMA reporting instructions. This represents a significant drop in the Department's maturity rating from FY 2018 to FY 2019, from a Level 4 to a Level 1. We attribute DHS' regress in managing its information security program to a decision made by the former DHS CIO in October 2019 to [redacted] This has led to a lack of Coast Guard security metric data, which adversely affects numerous key activities within the Identify, Detect, and

Respond functions, such as risk management, weakness remediation, system inventory, incident reporting, and continuous monitoring. DHS' FY 2018 and FY 2019 ratings are summarized in Table 3.

Table 3. DHS' Maturity Levels for Each Cybersecurity Function in FY 2018 Compared to FY 2019

Cybersecurity Function	Maturity Level	
	FY 2018	FY 2019
1. Identify	**Level 4 – Managed and Measureable**	**Level 1 – Ad Hoc**
2. Protect	Level 4 – Managed and Measureable	Level 4 – Managed and Measureable
3. Detect	**Level 4 – Managed and Measureable**	**Level 1 – Ad Hoc**
4. Respond	**Level 4 – Managed and Measureable**	**Level 1 – Ad Hoc**
5. Recover	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented

Source: OIG analysis based on our FY 2018 report[10] and *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*

Coast Guard's FISMA Reporting

A change in Coast Guard's cybersecurity and FISMA reporting had a widespread, adverse impact on DHS' information security program, practices, and rating, based on the maturity model approach outlined in the FY 2019 Inspector General FISMA reporting metrics and NIST's Cybersecurity Framework. Specifically, on June 11, 2019, [redacted]

The ramifications from this decision are two-fold because now, unlike other DHS components, [redacted]:

[redacted]

[10] *Evaluation of DHS' Information Security Program for Fiscal Year 2018,* OIG-19-60, September 19, 2019.

[11] The DHS CIO departed from DHS on November 15, 2019.

[12] As one of the five Armed Services of the United States, the Coast Guard is the only military branch within DHS. The Coast Guard operates under DHS during peacetime, and can be transferred to the Department of the Navy within DoD by the President at any time, or by the U.S. Congress during times of war. Congressional authority transfers happened twice: in 1917, during World War I, and in 1941, during World War II.

[redacted]

2. [redacted]

According to the former DHS CIO, the decision to allow [redacted] According to the former DHS CIO, he was not required to consult with the Deputy Under Secretary for Management due to a delegation of authority, per (44 United States Code (U.S.C.) § 3554(a)(3)) and Delegation 04000, which gives the DHS CIO authority to implement FISMA responsibilities for the Department.

In October 2019, the former DHS CISO informed OIG that the former CIO consulted with OMB before making the decision. According to a May 2, 2019 email, the former Federal CISO informally agreed with the need to eliminate the Coast Guard's dual FISMA reporting and was comfortable with including Coast Guard's metrics in DoD's submission. In addition, the former Federal CISO indicated it would leverage the Coast Guard's reporting as an opportunity for DoD to pilot a phased approach to complying with government-wide reporting requirements.

However, the former DHS CIO made the decision to change the reporting structure without consulting the Department's senior leadership or appropriate congressional oversight committees. Moreover, the CIO's decision is contrary to statutory reporting requirements under FISMA 2014, OMB's FY 2019 FISMA reporting instructions, and the terms stipulated in DHS senior leadership agreements with Coast Guard and DoD.[13] Reporting Coast Guard's information technology (IT) investment through DHS allows OMB to properly identify the costs of providing IT security as part of the Department's investment life cycle and to identify IT security costs for supporting infrastructure-related investments under FISMA.

[13] FISMA 2014 and OMB policy require agency CIOs to report annually to the agency head on the effectiveness of the agency's information security program, including progress of remedial actions. OMB requires that a plan of action and milestones (POA&M) contain a detailed resource estimate for accomplishing remedial actions, linked to the agency's budget submission.

It should also be noted that the DHS Under Secretary for Management and the Vice Commandant of the Coast Guard had previously drafted and signed a formal agreement in 2016 to ensure continued compliance of cybersecurity requirements. Coast Guard was expected to comply with all DHS FISMA monthly, quarterly, and annual reporting requirements, including providing incident reports. Specifically, the September 19, 2016 agreement stated that DHS would:

1. [redacted], and
2. require Coast Guard to meet all of its FISMA reporting obligations according to DHS FISMA reporting requirements designed to satisfy monthly, quarterly, and annual Congressional reporting to OMB.

Subsequently, a January 2017 agreement signed by the Secretaries of Defense and Homeland Security directed the [redacted] while also complying with DHS oversight and compliance requirements for acquisition, FISMA, and financial audit reporting. According to this 2017 agreement, this arrangement could be amended by mutual agreement, in writing, by the Secretaries of both Departments.

We contacted [redacted] personnel as part of this review. The [redacted] does not audit the Coast Guard as part of its annual FISMA review. Further, [redacted] personnel stated the DoD CIO does not follow the approved reporting metrics for its FISMA reporting. Instead, DoD's annual FISMA report is classified and is delivered to the appropriate congressional oversight committees. [redacted]

The absence of complete information security reporting from the Coast Guard has widespread ramifications for DHS' information security program. For example, [redacted]

[redacted]

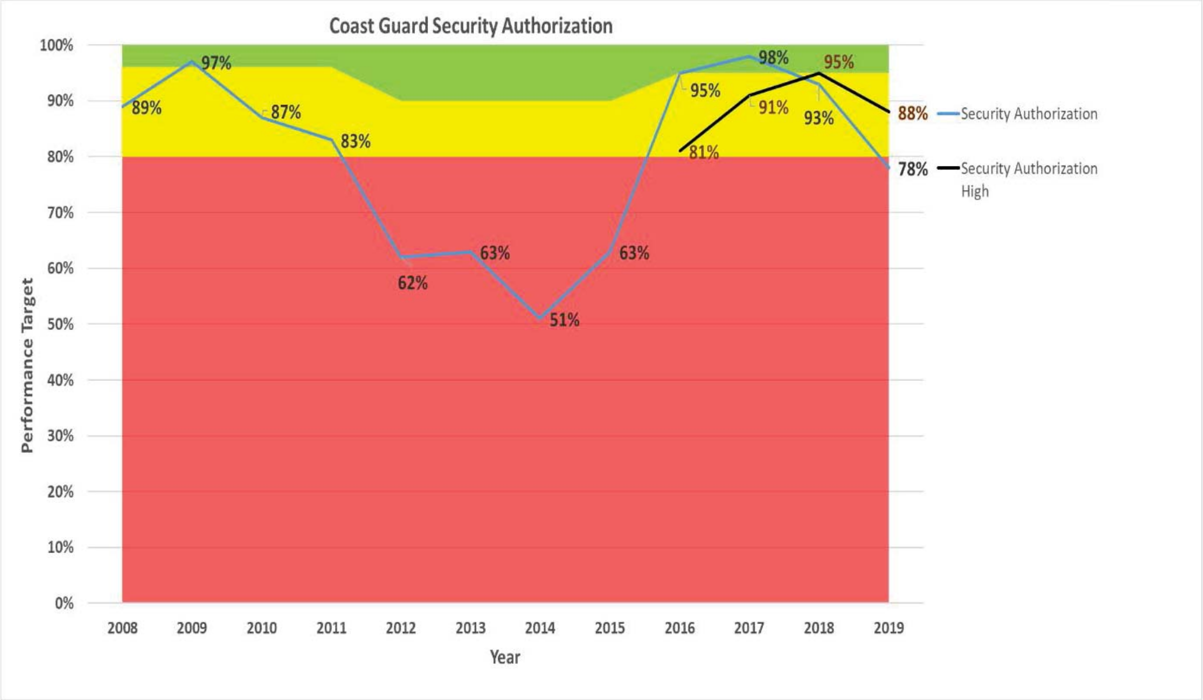
[redacted] We also have no assurance the former DHS CIO made a risk-based decision. On the contrary, the decision has adversely affected the Department's information security program in five key areas: risk management, weakness remediation, continuous monitoring, CDM, and incident reporting, as outlined in the following paragraphs.

Risk Management. As of the May 2019 scorecard, [redacted]

[14] NIST defines security authorization as the official management decision given by a senior official to authorize operation of a system. This is also known as an "authority to operate" (ATO).

[15] Per OMB guidance, agencies must create a remediation action plan (i.e., a POA&M for all known information security weaknesses, to identify and assess information system security and privacy weaknesses, set priorities for addressing them, and monitor progress toward mitigating them. To promote greater attention to security as a fundamental management priority, OMB works to integrate security in the capital planning and budget process. OMB also requires agencies to include unique project identifiers on the POA&Ms and the estimated security costs to remediate weaknesses.

Figure 1. Coast Guard Performance in Meeting the Authority to Operate Goal



Source: OIG analysis of DHS' June FISMA Scorecard between 2008 and 2019

Weakness remediation. Lacking Coast Guard data, DHS officials cannot examine consolidated POA&M information to identify common weaknesses or deficiencies across all Department information systems and propose or request solutions. When aggregated POA&M information is not available, DHS officials cannot allocate risk mitigation resources organization-wide and make adjustments to the Department's continuous monitoring strategy, as recommended by NIST. We reviewed DHS' June scorecards from 2008 to 2019 and determined the [redacted] during that period. As shown in Figure 2, [redacted]

[redacted]

[redacted]

[redacted]

Continuous Monitoring. [redacted] According to NIST Special Publication 800-137, the CISO establishes, implements, and maintains the organization's continuous monitoring program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; and consolidates and analyzes POA&Ms to determine organizational security weaknesses and deficiencies.

Consistent with our prior FISMA report findings, the absence of data from an individual DHS component results in a significant deficiency for the Department's overall information security program. Effective practices for continuous monitoring of the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cyber priorities are contingent on the CISO's ability to maintain an enterprise view.[16]

<u>DHS' Implementation of the Federal CDM Program</u>. CISA is primarily responsible for fulfilling DHS' national, non-law enforcement cybersecurity missions. It also provides crisis management, incident response, and defense

[16] *Evaluation of DHS' Information Security Program for Fiscal Year 2014,* OIG-15-16, December 12, 2014.

against cyberattacks for Federal executive branch networks (.gov) in civilian agencies. Failure to consult with the Department's senior leadership and OMB on whether the Coast Guard should participate in DHS' CDM Program may affect CISA's implementation of the CDM Program across the U.S. Government.

[redacted] According to the DHS Under Secretary for Management's 2016 agreement with the Coast Guard, the Coast Guard was expected to comply with all DHS FISMA monthly, quarterly, and annual reporting requirements, including providing incident reports. However, [redacted]

DHS' FY 2019 FISMA Ratings

Following is a complete discussion of all progress and deficiencies we identified in each cybersecurity function we evaluated, based on the maturity model approach outlined in the FY 2019 Inspector General FISMA reporting metrics and NIST's Cybersecurity Framework.

1. Identify

The "Identify" function requires developing an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. Per the FY 2019 FISMA reporting metrics, we determined that DHS was operating at "Level 1 – Ad Hoc" in this function. We based this rating on our conclusion that [redacted]

[redacted]

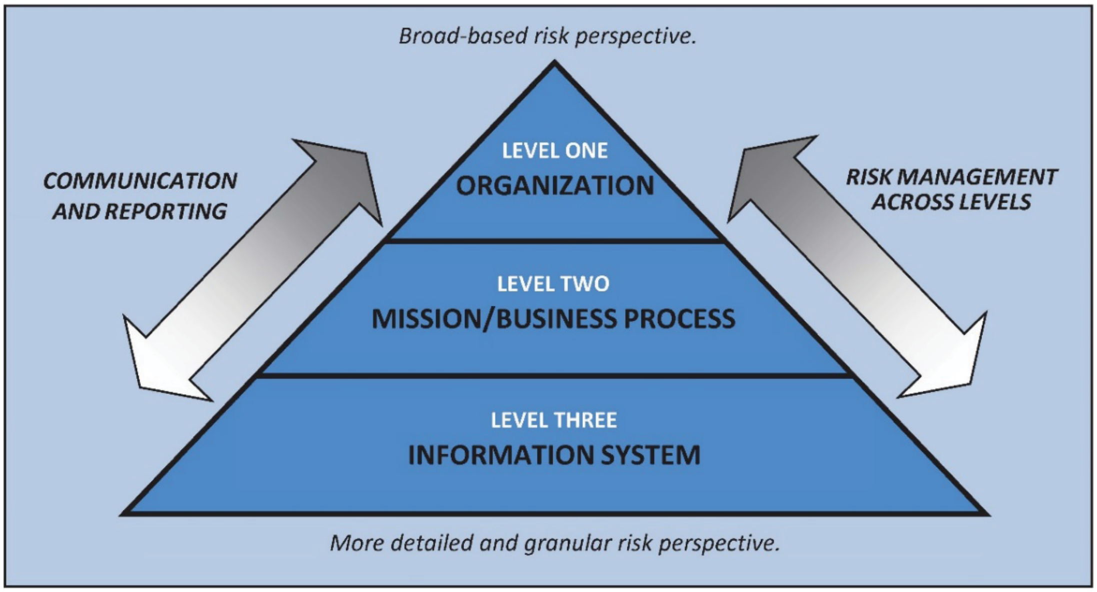
[redacted]

[redacted]

Risk Management

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization — from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level managers planning, executing, and managing projects; to individual users operating information systems supporting the organization's missions and business functions. Risk management requires that organizations: (1) establish the framework for risk-based decisions; (2) assess risk; (3) respond to risk once determined; and (4) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Therefore, risk management affects every aspect of the organization, including mission and business planning activities, the enterprise architecture, system development processes, and systems engineering activities integral to system life cycle management processes. Figure 3 illustrates a multi-level approach to risk management that addresses communication and reporting of security and privacy risk at the organization level, the mission/business process level, and the information system level.

Figure 3. Organization-Wide Risk Management Approach


Broad-based risk perspective.
COMMUNICATION AND REPORTING
LEVEL ONE
ORGANIZATION
RISK MANAGEMENT ACROSS LEVELS
LEVEL TWO
MISSION/BUSINESS PROCESS
LEVEL THREE
INFORMATION SYSTEM
More detailed and granular risk perspective.

Source: NIST Special Publication 800-37, Revision 2, December 2018

Risk management also encompasses the authorization process by which a senior management official (i.e., the authorizing official) reviews security and privacy information describing the current security and privacy posture of information systems.[17] The authorizing official uses this information to determine whether the mission/business risk of operating a system is acceptable and, if it is, explicitly accepts the risk by granting the system ATO. According to applicable DHS, OMB, and NIST policies, all systems must undergo the authorization process before they become operational.

DHS components are required to use enterprise management systems that incorporate NIST security controls when performing security assessments of their systems. Enterprise management systems enable centralized storage and tracking of all documentation required for the authorization package of each system. The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of the information system. Seven artifacts must be included in the ATO package:

1. privacy threshold analysis and, if required, privacy impact assessment

[17] A Federal information system is an information system used or operated by an executive agency, a contractor of an executive agency, or another organization on behalf of an executive agency.

2. security plan
3. contingency plan
4. security assessment plan
5. contingency plan test
6. security assessment report
7. authorization decision letter

Based on OMB and NIST guidance,[18] system ATOs are typically granted for a specific period in accordance with terms and conditions established by the authorizing official. In October 2013, DHS began allowing its components to enroll in an ongoing authorization program established by NIST. For each system to be admitted to the ongoing authorization program, a component must have a strong continuous monitoring process, approved common controls, a designated ongoing authorization manager, and a chartered organizational risk management board. In addition, DHS requires components to maintain security authorization and weakness remediation metrics above 60 and 80 percent, respectively, on the monthly FISMA Scorecard. After a component is accepted to the ongoing authorization program, system owners must fulfill the following requirements for each individual system:

- Ensure the component's enrollment in the ongoing authorization program is documented in the component's acceptance letter.
- Submit an admission letter to enroll the system in the ongoing authorization program.
- Receive an ongoing authorization recommendation letter from the Department to enroll the system in the ongoing authorization program.
- Ensure the system's ATO does not expire for at least 60 days when applying to enter the program.
- Assign the information system security officer with responsibilities primarily related to information assurance/security.
- Provide the information system security officer with training about ongoing authorization processes.
- Maintain an approved control allocation table listing the system security controls the component agrees to implement.

DHS maintains a target goal of ensuring ATOs for 100 percent of its 150 high-value systems assets.[19] The ATO target goal is 95 percent for its 373 operational non-high value assets. [redacted]

[18] OMB Circular A-130*, Managing Information as a Strategic Resource,* July 2016; NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 2018.
[19] High-value systems are those that may contain sensitive data used in DHS' critical operations or contain unique data that would make them of particular interest to attackers.

[redacted]

[redacted]

[redacted]

[redacted]

In addition, according to DHS' August 2019 FISMA scorecard, [redacted]

[redacted]

[redacted]

[redacted]

To determine the components' compliance in meeting DHS' NSS security authorization target, we examined the Department's August 2019 NSS Scorecard. We found that all components met the ATO target of 95 percent for their NSS systems, scoring 100 percent each. For NSS, this is an improvement over the seven classified systems that lacked ATOs in 2018.

Although we reported steady improvement with fewer unclassified systems operating without ATOs from FY 2016 to FY 2018, the total number of unclassified systems operating without ATOs has more than tripled since then, from FY 2018 to FY 2019. Our June 30, 2019 analysis of DHS' unclassified enterprise management system revealed [redacted] Table 4 outlines the number of unclassified systems operating without ATOs at selected components from FY 2016 to FY 2019.

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Source: OIG-compiled based on our analysis of data obtained from DHS' unclassified enterprise management system and our *Evaluation of DHS' Information Security Program for Fiscal Year 2017*, OIG-18-56, March 1, 2018; *Evaluation of DHS' Information Security Program for Fiscal Year 2018*, OIG 19-60, September 19, 2019

Weakness Remediation

FISMA requires the use of POA&Ms to track and plan the resolution of information security weaknesses. A POA&M details the resources required to

[20] *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, OIG-17-24, January 18, 2017; *Evaluation of DHS' Information Security Program for Fiscal Year 2017*, OIG-18-56, March 1, 2018; *Evaluation of DHS' Information Security Program for Fiscal Year 2018*, OIG-19-60, September 19, 2019.

accomplish elements of the plan, any milestones for meeting tasks, and scheduled completion dates for milestones.[21]

We found several components did not effectively manage the POA&M process as required by DHS. For example, although DHS requires components to update POA&Ms monthly, not all components consistently maintained complete and accurate information on progress in remediating security weaknesses. They also did not resolve all POA&Ms within 6 months as required, or consistently include estimates for resources needed to mitigate identified weaknesses. Our analysis of data from DHS' enterprise management system as of June 30, 2019, showed the following deficiencies:

- [redacted]
- [redacted]
- [redacted] DHS requires that components include a nominal weakness remediation cost of $50 when the cost cannot be estimated due to the complexity of tasks or other unknown factors.

Our analysis of the August 2019 *NSS FISMA Cybersecurity Scorecard* revealed only DHS Headquarters did not meet DHS' NSS weakness remediation metrics for POA&Ms.

2. Protect

The "Protect" function entails developing and implementing the appropriate safeguards to ensure delivery of critical services. It includes four FISMA domains: (1) Configuration Management, (2) Identity and Access Management, (3) Data Protection and Privacy, and (4) Security Training. We determined that, based on a simple majority as prescribed in the FY 2019 reporting metrics, DHS was operating at the target "Level 4 – Managed and Measureable" as the Department had effective practices to manage three of the four domains essential to the "Protect" function.

DHS can further improve its focus on key configuration management activities, such as replacing unsupported operating systems and timely application of security patches. We determined that some components we reviewed did not

[21] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

replace or update one unsupported operating system and did not apply security patches and updates timely to mitigate critical and high-risk security vulnerabilities on selected systems. In addition, components did not implement all configuration settings required to protect their systems. DHS components' compliance in each domain is described in the following paragraphs.

Configuration Management

We determined DHS was operating at "Level 1 - Ad Hoc" in the Configuration Domain, [redacted] Without Coast Guard information, DHS does not have an effective, enterprise-wide flaw remediation process for identifying, reporting, and correcting security vulnerabilities for all of its systems, including high-value assets or mission-essential systems.

DHS requires components to configure their Windows 10 workstations according to configuration settings set forth in DISA's Security Technical Implementation Guides. These settings are necessary to ensure confidentiality, integrity, and availability of DHS' systems and the information they process and store. To outline risk to information, the Defense Information Systems Agency ranks each setting/control in the Security Technical Implementation Guides as either Category I, II, or III. For example, if a Category I control is unimplemented or subverted, the risk to information is direct and immediate loss of confidentiality, integrity, or availability.

Our testing revealed that not all components we reviewed had implemented all required configuration settings. Specifically, we tested selected unclassified Windows 10 workstations at Coast Guard, FEMA, and USCIS to determine compliance with the required DISA's Security Technical Implementation Guides Category I settings. Table 5 summarizes the components' compliance.

Table 5. Selected Component Systems' Compliance with DISA's Security Technical Implementation Guides Category I Settings

Component	Percentage of Compliance
Coast Guard	96%
FEMA	91%
USCIS	100%

Source: OIG-compiled based on test results for three DHS components

The missing settings on the workstations we tested related to configuration of encryption algorithms, operating systems, and network communication. When these settings are not applied, unauthorized users can potentially access or exploit sensitive information. We found missing settings related to:

- Data Execution Prevention - Misconfiguration of this setting may allow harmful code to run in protected memory locations reserved for Windows and other programs.
- Structured Exception Handling Overwrite Protection - Misconfiguration of this setting may allow exploits that use the Structured Exception Handling overwrite technique — a common buffer overflow attack.

In a memorandum dated June 25, 2019, DHS allowed its components 135 days to transition to using DISA's Security Technical Implementation Guides, or to create and submit a system-level POA&M for each noncompliance. According to the *FY 2019 Information Security Performance Plan*, Version 1.6, dated July 5, 2019, [redacted]

Without implementing all proper configuration settings, components may render sensitive information stored on components' systems subject to potential exploitation. DHS can further improve its key configuration management activities by replacing unsupported operating systems and applying security patches.

Unsupported Operating Systems

Known or new vulnerabilities can be exploited on operating systems for which vendors no longer provide software patch updates or technical support. DHS requires components discontinue the use of such unsupported operating systems (e.g., Windows XP, Windows Server 2003). [redacted] Microsoft stopped providing technical support on this version of the operating system in April 2019.

Vulnerability Assessment Testing

Periodic scanning and assessment of critical systems is key to mitigating information security vulnerabilities. Per DHS guidance, components must reduce system vulnerabilities through testing, prompt installation of software patches, and elimination or disabling of unnecessary services. We performed vulnerability assessments at Coast Guard, FEMA, and USCIS. Table 6 summarizes the missing critical and high-risk software patches we identified.

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

If successfully exploited, these vulnerabilities could result in significant data loss or system disruption. Successful exploitation of critical and high-risk vulnerabilities may take the form of remote code execution, unauthorized modification or disclosure of information, or possible escalation of access rights and privileges. Ultimately, such exploitation could pose substantial risks to components' ability to carry out mission-critical DHS operations.

Identity and Access Management

Identity and access management is critical to ensure that only authorized users can log onto DHS systems. [redacted] pursuant to Homeland Security Presidential Directive-12.[22] DHS requires all privileged and unprivileged employees and contractors to use the cards to log onto DHS systems.

Per the FY 2019 FISMA reporting metrics, [redacted]

Data Protection and Privacy

DHS developed a data privacy policy in 2011 for the protection of PII stored and processed by its information systems. The DHS Privacy Office is responsible for privacy compliance across the Department, including ensuring the technologies used sustain and do not erode privacy protections for personal and departmental information.

[redacted]

[redacted]

Security Training Program

Educating employees about acceptable practices and rules of behavior is critical for an effective information security program. DHS has a security training program in place that is collaboratively managed by DHS

[22] *Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004, required Federal agencies to begin using a standard form of identification to gain physical and logical access to federally controlled facilities and information systems.

Headquarters, the Office of the Chief Human Capital Officer, and the components. Specifically, the Department uses a Performance and Learning Management System to track employee completion of training, including security awareness courses. Components are required to ensure all employees and contractors receive annual IT security awareness training, as well as specialized training for employees with significant responsibilities.

However, DHS did not provide documentation to support that its security awareness and training program was properly resourced per the FY 2019 FISMA reporting metrics. Further, according to the program officials we met with, while DHS assessed the knowledge, skills, and abilities of its cyber workforce, it has not finalized a strategy to address identified gaps outlined in its Cybersecurity Workforce Assessment. Without a workforce strategy, DHS cannot assure that its employees possess the knowledge and skills necessary to perform job functions, or that qualified personnel are hired to fill cybersecurity-related positions.

Although the Department has made overall progress in the "Protect" function, DHS components can further safeguard the Department's information systems and sensitive data by:

- implementing all required configuration settings;
- discontinuing use of unsupported operating systems;
- applying security patches timely;
- establishing qualitative and quantitative measures to monitor data exfiltration or enhanced network defenses; and
- finalizing a Cybersecurity Workforce strategy to address identified gaps outlined in its assessment.

3. Detect

The "Detect" function entails developing and implementing appropriate activities, including ongoing systems authorization and continuous monitoring, to identify any irregular system activity. Per the FY 2019 FISMA reporting metrics, we determined that DHS was operating at "Level 1 – Ad Hoc" in this function as the Department did not have an effective strategy and organization-wide ISCM approach to address all requirements and activities at each organizational tier.

According to NIST, an effective ISCM program should begin with the development of a comprehensive strategy that addresses ISCM requirements and activities at each organizational tier (organization, mission/business processes, and information systems), and include metrics that provide meaningful indications of security status at all organizational tiers. However, DHS relied on data calls via email to maintain visibility into each component's national security systems, instead of using the enterprise management tool or other information validation procedures that create security artifacts for monitoring and authorizing each system. In addition, DHS did not establish an ongoing authorization program for its national security systems.

As of June 2019, eight components were enrolled in the Department's ongoing authorization program. The Department had increased the number of systems enrolled in the program from FY 2017 to FY 2019, as shown in Figure 6.

[redacted]

[redacted]

Information Security Continuous Monitoring (ISCM)

As part of the Detect function, DHS established its continuous monitoring, or ISCM, program, which allows officials to gain visibility into network resources, maintain awareness of security threats and vulnerabilities, and ensure effectiveness of implemented controls. In 2011, DHS developed an initial ISCM strategy. DHS' current ISCM program for its unclassified systems includes monthly data feeds from automated system scans performed across component networks and systems. [redacted]

- [redacted]
- [redacted]
- [redacted]

Our analysis of DHS' August 2019 *NSS FISMA Cybersecurity Scorecard* revealed that while five components — CISA, FEMA, S&T, USCIS, and TSA — received 100 percent scores for contingency plan testing, [redacted]

4. Respond

The "Respond" function entails developing and implementing appropriate responses to detected cybersecurity events. We determined that DHS was operating at "Level 1 – Ad Hoc" in this function as the [redacted]

Incident Response

According to FISMA 2014, an "incident" is an occurrence that jeopardizes or may jeopardize the integrity, confidentiality, or availability of information or an information system without legal consent. It may also constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Although agencies can reduce the frequency of incidents by taking actions and instituting controls to secure their networks and systems, they have no assurance of preventing all incidents.

The Department established two Security Operation Centers to monitor and respond to suspicious activities — one for unclassified systems and the other for classified systems. These Security Operations Centers are responsible for ensuring components comply with applicable Federal and DHS security policy and corresponding controls. DHS Security Operations Centers provide situational awareness, serve as central data repositories, and facilitate reporting and coordination regarding computer security incidents across the Department. In addition, DHS personnel are required to follow DHS Security

Operations Center procedures for detecting, reporting, and responding to information security incidents.[23]

The "Respond" function supports agencies' ability to contain the impact of a potential cybersecurity event. As such, the function not only requires agencies to develop procedures for detecting, reporting, and responding to security incidents, it also requires coordinating response activities with internal and external stakeholders. Specifically, FISMA 2014 requires agencies to:

- notify and consult with law enforcement agencies and relevant Offices of Inspector General and General Counsel, as appropriate; and
- inform selected congressional oversight committees of major incidents within the required timeframe.

[redacted]

Given agencies' increased reliance on computer resources to accomplish their missions, incident response has become a vital part of an effective information security program. When security incidents are not reported to the Security Operations Centers, the Department cannot take appropriate corrective actions to contain their potential impact and protect against a potential cybersecurity event. Moreover, the Security Operations Centers may lack the information they need to address suspicious activity as quickly as possible.

<u>Major Incidents</u>

In FY 2019, DHS reported two major incidents. According to applicable FISMA major incident reporting requirements, the Department notified selected congressional oversight committees of the following:

[23] DHS' incident response procedures are outlined in 4300A, 4300B, and 4300C.

[redacted]

5. Recover

DHS' approximately 240,000 employees rely heavily on information technology to perform their duties. Because information systems and resources are so vital to DHS' accomplishment of its mission operations, it is critical to minimize the effect of service interruptions and avoid extensive outages in the event of an emergency. The "Recover" function entails developing and implementing plans for resiliency and restoration of any capabilities or services impaired due to outages or other disruptions from a cybersecurity event.

We determined DHS' "Recover" function was operating at "Level 3 – Consistently Implemented," just below the targeted level for effectiveness. We based this rating on our assessment that [redacted] Although contingency planning is vital to agency recovery from a cybersecurity event, DHS' progress in this area was minimal from 2018 to 2019.

Contingency Planning

DHS has a department-wide business continuity program to react to emergency events, restore essential business functions, and resume normal operations. As part of this program, DHS implemented a Reconstitution Requirements Functions Worksheet to collect information on components' key business requirements and capabilities needed to recover from attack or

[24] On November 9, 2018, OIG issued a draft management alert to notify FEMA about the incident. Subsequently, OIG issued the final report, *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED),* OIG-19-32, on March 15, 2019.
[25] OIG began a review of this CBP incident in October 2019.

disaster. DHS used this information to develop a Reconstitution Plan that outlines procedures at a macro level for all DHS senior leadership, staff, and components to follow to resume normal operations as quickly as possible in the event of an emergency. The procedures may involve both manual and automated processing at alternate locations, as appropriate. DHS components are responsible for developing and periodically testing such contingency plans outlining backup and disaster recovery procedures for the respective information systems. However, as of June 30, 2019, we identified the following deficiencies:

[redacted]

[redacted]

DHS has made little progress, maintaining a "Level 3 – Consistently Implemented" rating in the "Recover" function for the past 3 years. A well-documented and tested contingency plan can ensure the recovery of critical network operations. Untested plans may create a false sense of security and an inability to recover operations in a timely manner.

Summary of Selected Components' Implementation of Information Security Programs

According to FY 2019 reporting metrics, our independent contractor rated component information security programs effective for CBP and ICE as both components achieved the targeted "Level 4 – Managed and Measurable" or higher in four of five functions. CISA's overall information security program was not effective because it achieved "Level 1 – Ad-hoc," which is below the targeted Level 4 in three of five functions. Because the Department performs several security functions on CISA's behalf, CISA has not yet developed component specific policies, procedures, and business processes as required by DHS policy. Table 7 summarizes CBP, CISA, and ICE's implementation of information security programs.

Table 7. Summary Status of CBP, CISA, and ICE's Information Security Programs for FY 2019

Function / Component	CBP	CISA	ICE
Identify	Level 5 – Optimized	Level 3 - Consistently Implemented	Level 5 - Optimized
Protect	Level 5 – Optimized	Level 1 - Ad-hoc	Level 4 - Managed and Measurable
Detect	Level 4 - Managed and Measurable	Level 3 - Consistently Implemented	Level 5 - Optimized
Respond	Level 4 - Managed and Measurable	Level 1 - Ad-hoc	Level 4 - Managed and Measurable
Recover	Level 3 - Consistently Implemented	Level 1 - Ad-hoc	Level 3 - Consistently Implemented
Overall Rating	Level 4 - Managed and Measurable	Level 1 - Ad-hoc	Level 4 - Managed and Measurable

Source: OIG contractor

Recommendations

We recommend the Deputy Under Secretary for Management:

Recommendation #1: Consider whether the former DHS CIO's May 2019 decision [redacted] was in compliance with the terms outlined in the 2016 and 2017 agreements established by both Departments' senior leadership, as well as all applicable statutory reporting requirements under FISMA and OMB reporting requirements, and update the agreement, where appropriate.

Recommendation #2: Assess the risk posed to the Department's information security program [redacted], inform DHS senior leadership of the risks identified, document senior leadership's concurrence or non-concurrence with the former CIO's decision, and communicate the decision, in writing, to OMB and selected congressional oversight committees.

We recommend the DHS CIO:

Recommendation #3: Revise the Department's information security policies to reflect senior leadership's approval and any revisions regarding [redacted]

Recommendation #4: Enforce requirements for components to obtain authority to operate, test contingency plans, and apply sufficient resources to mitigate security weaknesses for both their unclassified systems and NSS.

We recommend the CISA CIO:

Recommendation #5: Strengthen the component's information security program by establishing necessary policies and procedures according to the NIST Cybersecurity Framework.

Management Comments and OIG Analysis

DHS concurred with all five of our recommendations. A copy of DHS' response in its entirety is included in Appendix B. DHS also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate.

We obtained written comments on a draft of this report from the Director of the Departmental GAO-OIG Liaison Office. In the comments, the Director of the Departmental GAO-OIG Liaison Office stated the Department appreciates the work of OIG in planning and conducting its review and issuing this report. Following is our evaluation of the Department's general comments, as well as a response to each recommendation in the draft report provided for agency review and comment.

OIG Response to General Comments:

- The Director of the Departmental GAO-OIG Liaison Office stated DHS does not agree with OIG's overall FY 2019 FISMA rating of "not effective" due to the specific ratings of "Ad Hoc" (Level 1) received in the "Identify," "Detect," and "Respond" areas of the report. We note that FISMA requires each OIG to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. According to the FY 2019 OIG reporting metrics, OIGs have the discretion to determine the overall effectiveness rating and rating for each of the Cybersecurity Framework functions at the maturity level of their choosing.

Using this approach, the OIG may determine that a particular function area and/or the agency's information security program is effective at a maturity level lower than Level 4. As such, there is no requirement for the OIG to come into agreement with the CIO on the Department's effectiveness rating and the rating for each of the Cybersecurity Framework functions.

- Further, the Department disagrees with OIG's overall assessment that DHS regressed in the management of its information security program due to [redacted] The Director claimed our conclusion was primarily derived from the OIG's incorrect legal assessment that the CIO lacks the authority to make such a decision. We disagree with the Director's assertions and stand by our position. Specifically:

  - FISMA Section 3554 imposes on the head of DHS (subject to certain powers being delegable to the DHS CIO) the responsibility to provide information security protections for "information collected or maintained by or on behalf of the agency" and "information systems used or operated by an agency … or other organization on behalf of an agency." The statute does not include language to permit [redacted]

  - The head of DHS must comply with related policies, procedures, standards, and guidelines that apply agency-wide. Per Section 3554(a)(5), the head of DHS must ensure that the agency CIO "report[s] annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions." The head of DHS must also ensure that senior agency officials, including CIOs of component agencies, carry out their responsibilities and ensure that "all personnel are held accountable for complying with the agency-wide information security program…." Section 3554(b) spells out the requirement for an "agency-wide information security program" for "the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency." The head of DHS must then develop policies and procedures based on those risk assessments. The "agency-wide information security program" also includes requirements for security awareness training, periodic testing and evaluation (of all information systems in the agency's inventory), remedial action processes, security incident detection, reporting and response, and continuity of operations. Section 3554(c) imposes annual reporting requirements on the agency, including a description of each major information security incident (e.g., the risk assessments previously conducted on the affected systems and the status of compliance with security requirements at the time of the incident), the total number of information security incidents, and a description of each incident involving a breach of PII.

- In summary, FISMA imposes agency-wide responsibilities on the agency head and nothing in the statute permits the agency to [redacted] DHS appears to rely on Section 3554(a)(3)-(7) as providing discretion to allow the agency [redacted] However, although these provisions of the statute give limited discretion in certain other respects, nowhere does the statute provide authority for this decision. Section 3554(a)(3), of the statute, which the acting DHS CIO and Coast Guard rely upon in their May 26, 2020 Memorandum for the Acting Secretary of DHS, delegates to the CIO "the authority to ensure compliance with the requirements imposed on the agency under this subchapter." The authority to ensure compliance, however, does not expressly include the authority to [redacted]

- The Director of the Departmental GAO-OIG Liaison Office claimed "despite numerous meetings with Department and Component program officials, subject matter experts, and others, as well as the sharing of extensive supporting documentation, the OIG's audit team does not appear to understand that Coast Guard systems do not pose any significant cybersecurity risk to DHS or Coast Guard because they operate on [redacted]" We disagree. While the Director claimed the Department took the Congressional incident reporting responsibility seriously, we do not believe the FISMA statute gives agencies the discretion to [redacted]

- The Director of the Departmental GAO-OIG Liaison Office stated its concern over the OIG's conclusion that DHS FISMA reporting was deficient because of the Coast Guard's decision. Specifically, the Director claimed, "when making this assertion, the OIG's draft report provides few specifics, and does not cite any specific responsibility that is not being met." We find this assertion inconsistent with our report, which clearly outlines specific reasons why DHS' FISMA reporting to Congress is deficient. Primarily, according to page 7 of our report, the ramifications from this decision include that the [redacted]:

1. [redacted]

2. [redacted]

- We encourage the Department to consider the additional potential risks stemming from this reporting decision. For example, a DoD IG official informed us [redacted]

- The Director of the Departmental GAO-OIG Liaison Office stated, "DHS OCIO continues to work with Coast Guard, and their data continues to reside within the DHS compliance tool." The Director requested we communicate [redacted] the importance that it take responsibility for evaluating [redacted] systems as required under FISMA. We disagree with this request because (1) we believe there is no statutory basis for [redacted] and (2) it suggests we need to abdicate our Coast Guard oversight responsibility. Nevertheless, it should be noted we did reach out to [redacted] to discuss [redacted] As stated previously, [redacted]

- As the Departmental GAO-OIG Liaison recognized in his memo, both we and the Department aim to achieve the right balance between addressing sensitivity concerns and the need to inform Congress and the public.

Response to Report Recommendations:

In the formal written comments, the Director of the Departmental GAO-OIG Liaison Office concurred with all five recommendations. Following is a summary of DHS' response to each recommendation and the OIG's analysis.

DHS Comments to Recommendation #1: Concur. DHS stated the [redacted] FISMA recognizes DHS as the operational lead for Federal cybersecurity and has the authority to coordinate government-wide cybersecurity efforts, issue binding operational directives detailing actions agencies should take to improve their cybersecurity, and provide operational and technical assistance to agencies, including through the operation of the Federal information security incident center. More specifically, the CIO has been delegated senior authority and oversight of the development and maintenance of the DHS-wide information security program, including assisting DHS component senior officials concerning their responsibilities.

DHS indicated [redacted] The former CIO then contacted the OMB CISO on May 2, 2019, who agreed it was best to eliminate dual FISMA reporting experienced by [redacted] The decision was in accordance with FISMA (44 USC § 3554) and the *Federal Information Security Modernization Act of 2014*, "Annual Report to Congress." The OMB CISO concurred that reporting [redacted] metrics to OMB as part of DoD's submission was acceptable. [redacted] continues to provide monthly FISMA reports, and the DHS OCIO/CISO Cybersecurity Risk Management and Compliance Division continuously reviews them monthly, enabling DHS OCIO senior leadership to assess and evaluate potential risks to the Department's Information Security programs. DHS requested OIG consider this recommendation resolved and closed, as implemented.

OIG Analysis of DHS Comments: DHS did not fully address this recommendation. We maintain the FISMA statute mandates an agency-wide information security program and a requirement that all components provide [redacted]. Further, the Department did not discuss whether the former CIO's decision complied with the terms outlined in the 2016 and 2017 agreements between DoD and DHS. This recommendation will remain open and unresolved until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #2: Concur. DHS stated that during May 2019, the DHS OCIO conducted a risk assessment review to evaluate the connections between the [redacted] and DHS OneNet. The review confirmed that [redacted] systems are currently only operational on the [redacted], there is low risk to the DHS infrastructure and all operational risk acceptance resides with [redacted]. DHS also participated in a September [redacted] Lastly, OCIO conducted a second risk assessment review in November 2019 and learned that [redacted] uses and/or operates networks connected and operating [redacted] in the same manner that DHS uses and/or operates networks connected on the DHS OneNet. For example, [redacted] readiness, national security, and national defense missions, and also performs mission-critical activities during reliance on these networks as with DHS OneNet, in comparison. DHS requested OIG consider this recommendation resolved and closed, as implemented.

OIG Analysis of DHS Comments: We maintain that FISMA imposes agency-wide responsibilities on the agency head and nothing in the statute permits the agency to [redacted]. An inter-agency agreement cannot be used to avoid a statutory requirement. This recommendation will remain open and unresolved until DHS provides documentation to support that the Department's senior-most leadership has communicated its concurrence or non-concurrence with the former CIO's decision, in writing, to OMB and selected congressional oversight committees.

DHS Comments to Recommendation #3: Concur. DHS CIO authorizes the revision of DHS security policies to reflect the decision of the former CIO, [redacted] DHS Policy 4300A, *Sensitive Systems Policy Directive*, will be updated, particularly the sections on Performance Measurement and Metrics (3.4) and Required Reporting (3.13). Estimated Completion Date: January 29, 2021

OIG Analysis of DHS Comments: DHS' actions are responsive to this recommendation. This recommendation will remain open and resolved until

DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #4: Concur. During January 2015, the former CIO implemented processes and policies to ensure components obtain ATO and develop contingency plans, thereby authorizing operation of their systems and accepting the risk to agency operations. The testing involved, but was not limited to, periodic testing and evaluation of the effectiveness of information security policies, procedures, best practices, and was performed with a frequency depending on risk. Testing often entails management, operational, and technical controls for every information system identified in the inventory, as required. DHS OCIO established testing activities that continue as current processes and operations today.

The DHS CIO is also working with the DHS Office of the Chief Financial Officer to ensure components have adequate resources to mitigate security weaknesses for both unclassified and NSS. Specifically, the DHS CIO established a quarterly security training program, ensuring that all components have trained personnel able to assist in complying with requirements of FISMA and related OMB and DHS policies, procedures, standards, and guidelines. The DHS CIO continues to manage the Department's information security program and ensures continued coordination with DHS component senior agency officials. The DHS CIO also ensures annual reports are submitted as required, demonstrating effectiveness of the information security programs and including remedial corrective actions. Lastly, DHS OCIO publishes and maintains the annual Information Systems Cybersecurity Performance Plan, which communicates requirements, priorities, and overall Departmental Information Security goals for NSS and sensitive systems. DHS requested OIG consider this recommendation resolved and closed, as implemented.

OIG Analysis of DHS Comments: DHS' actions are responsive to the intent of this recommendation. However, DHS did not provide detailed procedures on enforcing the requirements for weakness remediation, contingency plan testing, and systems operating without ATOs. This recommendation will remain open and unresolved until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #5: Concur. DHS believes this recommendation was misdirected to the CISA CIO. Although CISA was only established on November 16, 2018, the DHS CIO is working with the CISA CIO to strengthen CISA's information security program, as well as its policies and procedures in accordance with NIST guidance and Department policies. Currently, the DHS CIO holds regular meetings with CISA on its information security program and the DHS CIO will work with CISA to develop a plan to make these improvements. Estimated Completion Date: September 30, 2021.

OIG Analysis of DHS Comments: We maintain we properly addressed this recommendation to the CISA CIO, who has been delegated authority for overseeing the development and maintenance of CISA's information security program and FISMA compliance. CISA is the Department's operational lead for government-wide Federal cybersecurity. Through coordination with OMB, the CIO Counsel, the OIG community, CISA developed the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* based on the NIST Cybersecurity Framework. However, our independent contractor rated CISA's information program as not effective, "Level 1 – Ad-hoc," because CISA has not yet developed component-specific policies, procedures, and business processes as required by DHS policy. We believe that, prior to its reorganization as CISA in 2018, the former National Protection and Programs Directorate should have developed policies and procedures based on the NIST Cybersecurity Framework model. The DHS CIO may assist CISA if the CIO determines it would be beneficial. This recommendation will remain open and unresolved until CISA provides documentation to support that all planned corrective actions are completed.

Appendix A
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*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote efficiency and effectiveness within the Department.

The objective of our evaluation was to determine whether DHS' information security program and practices adequately and effectively protect the information and information systems supporting DHS' operations and assets for fiscal year 2019. Our independent evaluation focused on assessing DHS' information security program against requirements outlined in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. Specifically, we evaluated DHS' information security program's compliance with requirements outlined in five NIST Cybersecurity Functions.

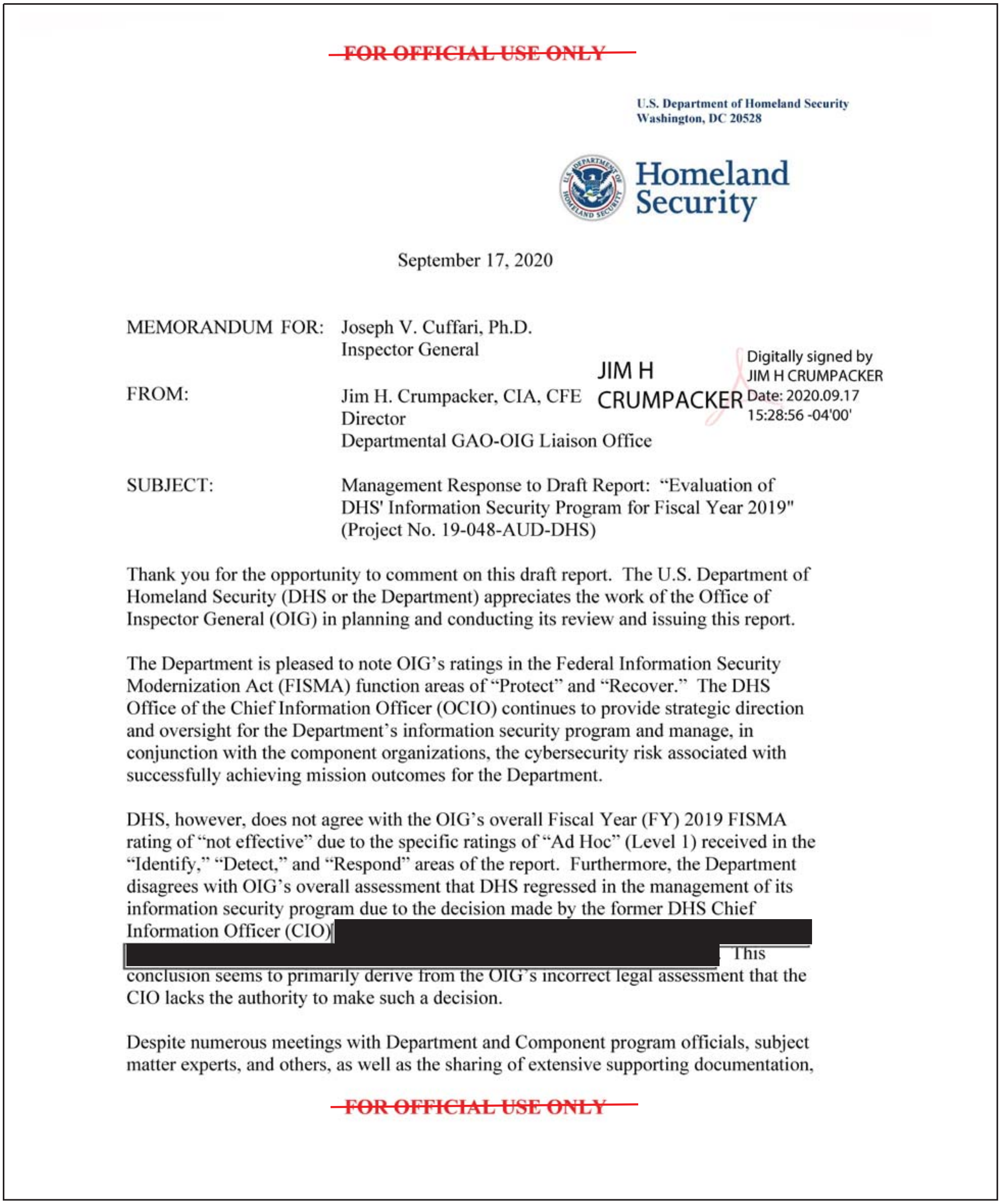
We performed our fieldwork at the DHS Office of the CISO and at selected organizational components and offices, including CISA, Coast Guard, Headquarters, CBP, FEMA, ICE, and USCIS. To conduct our evaluation, we interviewed relevant DHS Headquarters and component personnel, assessed DHS' current operational environment, and determined compliance with FISMA requirements and other applicable information security policies, procedures, and standards. Specifically, we:

- referenced our FY 2018 FISMA evaluation as a baseline for the FY 2019 evaluation;
- evaluated policies, procedures, and practices DHS had implemented at the program and component levels;
- reviewed DHS' POA&Ms and ongoing authorization procedures to determine whether security weaknesses were identified, tracked, and addressed;
- evaluated processes and the status of the department-wide information security program reported in DHS' monthly information security scorecards regarding risk management, contractor systems, configuration management, identity and access management, security training, information security continuous monitoring, incident response, contingency planning; and
- developed an independent assessment of DHS' information security program.

Using scanning tools, we conducted vulnerability assessments of controls implemented at three components. We tested DHS' compliance with applicable Defense Information Systems Agency's Security Technical Implementation Guides on selected Windows 10 workstations. We also reviewed information from DHS' enterprise management systems to determine data reliability and accuracy. We found no discrepancies or errors in the data. OIG contractors performed fieldwork at CBP, CISA, and ICE to support our evaluation.

We conducted this review between June and November 2019 under the authority of 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 did not evaluate OIG's compliance with FISMA requirements during our review.

Appendix B
Management Comments to the Draft Report



~~FOR OFFICIAL USE ONLY~~

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 17, 2020

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

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2020.09.17 15:28:56 -04'00'

SUBJECT: Management Response to Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2019" (Project No. 19-048-AUD-DHS)

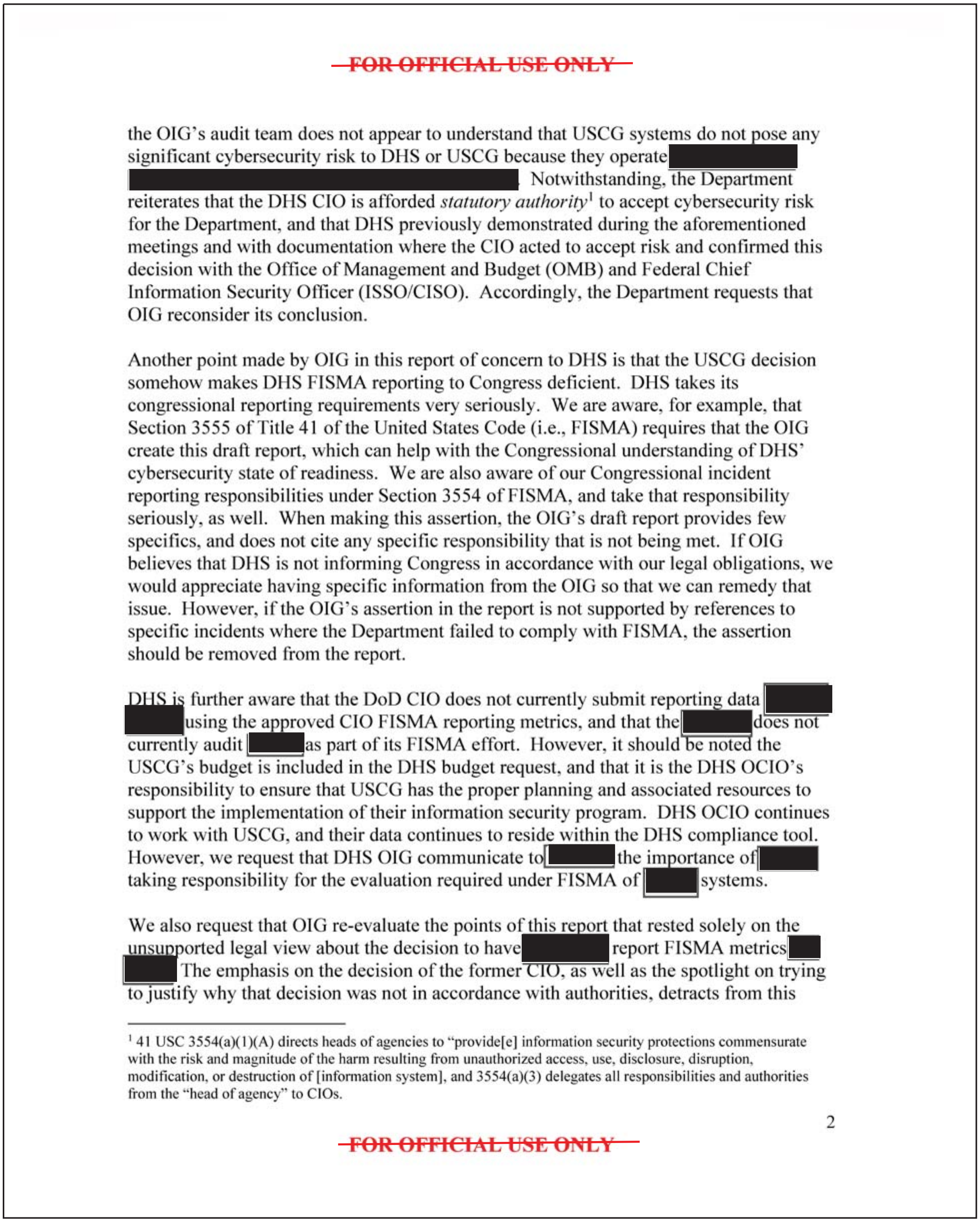
Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Department is pleased to note OIG's ratings in the Federal Information Security Modernization Act (FISMA) function areas of "Protect" and "Recover." The DHS Office of the Chief Information Officer (OCIO) continues to provide strategic direction and oversight for the Department's information security program and manage, in conjunction with the component organizations, the cybersecurity risk associated with successfully achieving mission outcomes for the Department.

DHS, however, does not agree with the OIG's overall Fiscal Year (FY) 2019 FISMA rating of "not effective" due to the specific ratings of "Ad Hoc" (Level 1) received in the "Identify," "Detect," and "Respond" areas of the report. Furthermore, the Department disagrees with OIG's overall assessment that DHS regressed in the management of its information security program due to the decision made by the former DHS Chief Information Officer (CIO) [redacted] This conclusion seems to primarily derive from the OIG's incorrect legal assessment that the CIO lacks the authority to make such a decision.

Despite numerous meetings with Department and Component program officials, subject matter experts, and others, as well as the sharing of extensive supporting documentation,

~~FOR OFFICIAL USE ONLY~~



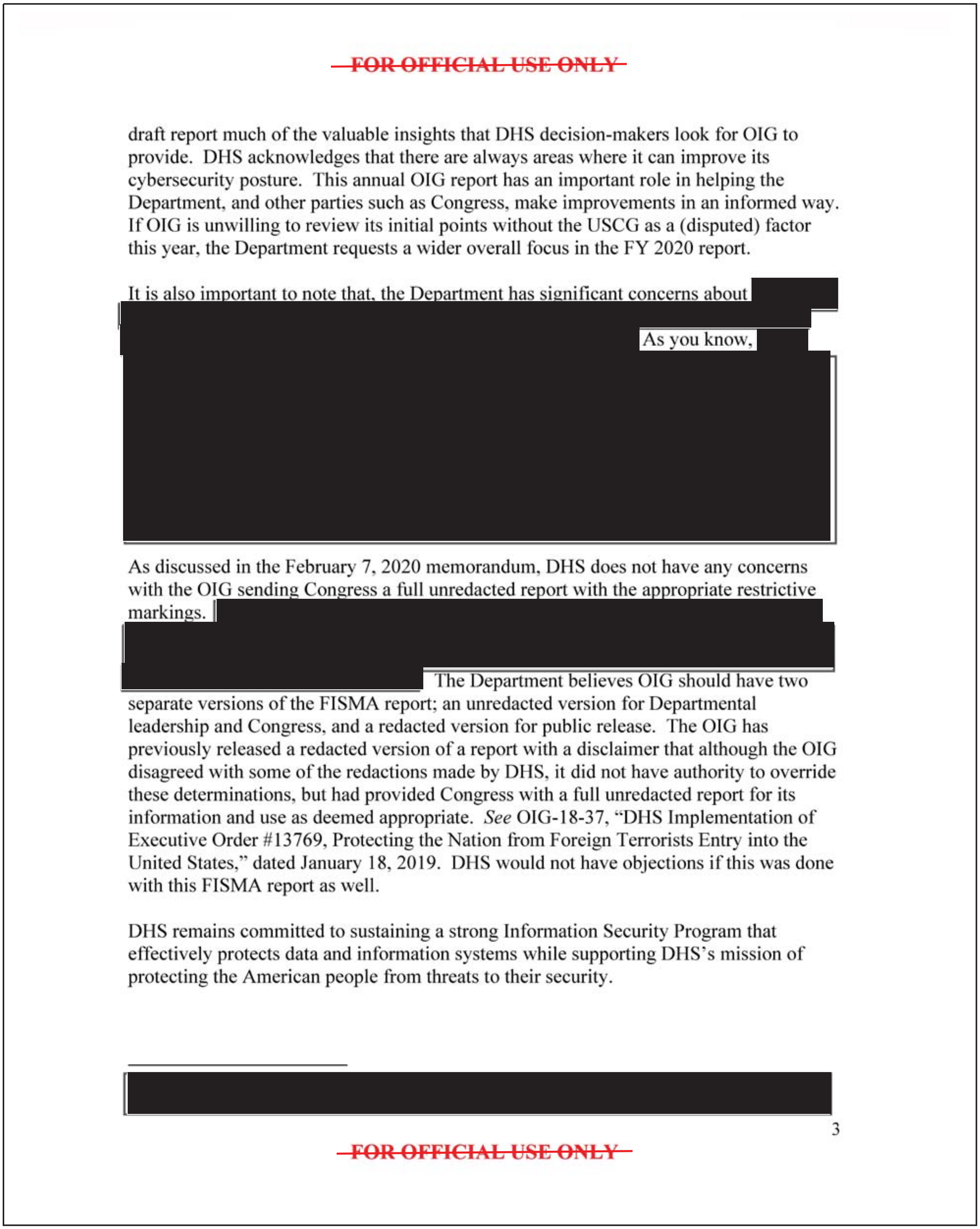
the OIG's audit team does not appear to understand that USCG systems do not pose any significant cybersecurity risk to DHS or USCG because they operate [redacted]. Notwithstanding, the Department reiterates that the DHS CIO is afforded *statutory authority*[1] to accept cybersecurity risk for the Department, and that DHS previously demonstrated during the aforementioned meetings and with documentation where the CIO acted to accept risk and confirmed this decision with the Office of Management and Budget (OMB) and Federal Chief Information Security Officer (ISSO/CISO). Accordingly, the Department requests that OIG reconsider its conclusion.

Another point made by OIG in this report of concern to DHS is that the USCG decision somehow makes DHS FISMA reporting to Congress deficient. DHS takes its congressional reporting requirements very seriously. We are aware, for example, that Section 3555 of Title 41 of the United States Code (i.e., FISMA) requires that the OIG create this draft report, which can help with the Congressional understanding of DHS' cybersecurity state of readiness. We are also aware of our Congressional incident reporting responsibilities under Section 3554 of FISMA, and take that responsibility seriously, as well. When making this assertion, the OIG's draft report provides few specifics, and does not cite any specific responsibility that is not being met. If OIG believes that DHS is not informing Congress in accordance with our legal obligations, we would appreciate having specific information from the OIG so that we can remedy that issue. However, if the OIG's assertion in the report is not supported by references to specific incidents where the Department failed to comply with FISMA, the assertion should be removed from the report.

DHS is further aware that the DoD CIO does not currently submit reporting data [redacted] using the approved CIO FISMA reporting metrics, and that the [redacted] does not currently audit [redacted] as part of its FISMA effort. However, it should be noted the USCG's budget is included in the DHS budget request, and that it is the DHS OCIO's responsibility to ensure that USCG has the proper planning and associated resources to support the implementation of their information security program. DHS OCIO continues to work with USCG, and their data continues to reside within the DHS compliance tool. However, we request that DHS OIG communicate to [redacted] the importance of [redacted] taking responsibility for the evaluation required under FISMA of [redacted] systems.

We also request that OIG re-evaluate the points of this report that rested solely on the unsupported legal view about the decision to have [redacted] report FISMA metrics [redacted] The emphasis on the decision of the former CIO, as well as the spotlight on trying to justify why that decision was not in accordance with authorities, detracts from this

[1] 41 USC 3554(a)(1)(A) directs heads of agencies to "provide[e] information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of [information system], and 3554(a)(3) delegates all responsibilities and authorities from the "head of agency" to CIOs.



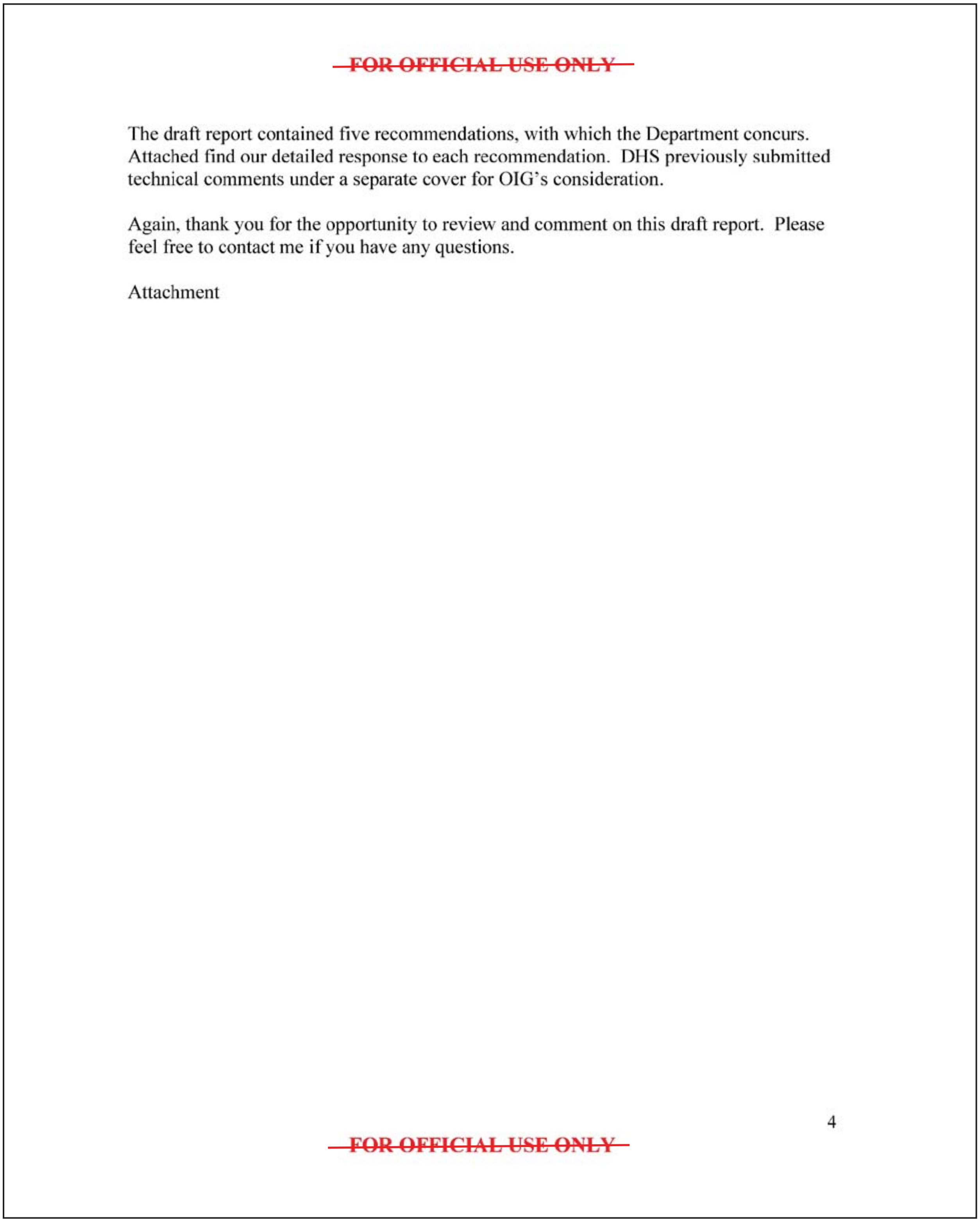
draft report much of the valuable insights that DHS decision-makers look for OIG to provide. DHS acknowledges that there are always areas where it can improve its cybersecurity posture. This annual OIG report has an important role in helping the Department, and other parties such as Congress, make improvements in an informed way. If OIG is unwilling to review its initial points without the USCG as a (disputed) factor this year, the Department requests a wider overall focus in the FY 2020 report.

It is also important to note that, the Department has significant concerns about [redacted] As you know, [redacted]

As discussed in the February 7, 2020 memorandum, DHS does not have any concerns with the OIG sending Congress a full unredacted report with the appropriate restrictive markings. [redacted] The Department believes OIG should have two separate versions of the FISMA report; an unredacted version for Departmental leadership and Congress, and a redacted version for public release. The OIG has previously released a redacted version of a report with a disclaimer that although the OIG disagreed with some of the redactions made by DHS, it did not have authority to override these determinations, but had provided Congress with a full unredacted report for its information and use as deemed appropriate. *See* OIG-18-37, "DHS Implementation of Executive Order #13769, Protecting the Nation from Foreign Terrorists Entry into the United States," dated January 18, 2019. DHS would not have objections if this was done with this FISMA report as well.

DHS remains committed to sustaining a strong Information Security Program that effectively protects data and information systems while supporting DHS's mission of protecting the American people from threats to their security.

[redacted]



~~FOR OFFICIAL USE ONLY~~

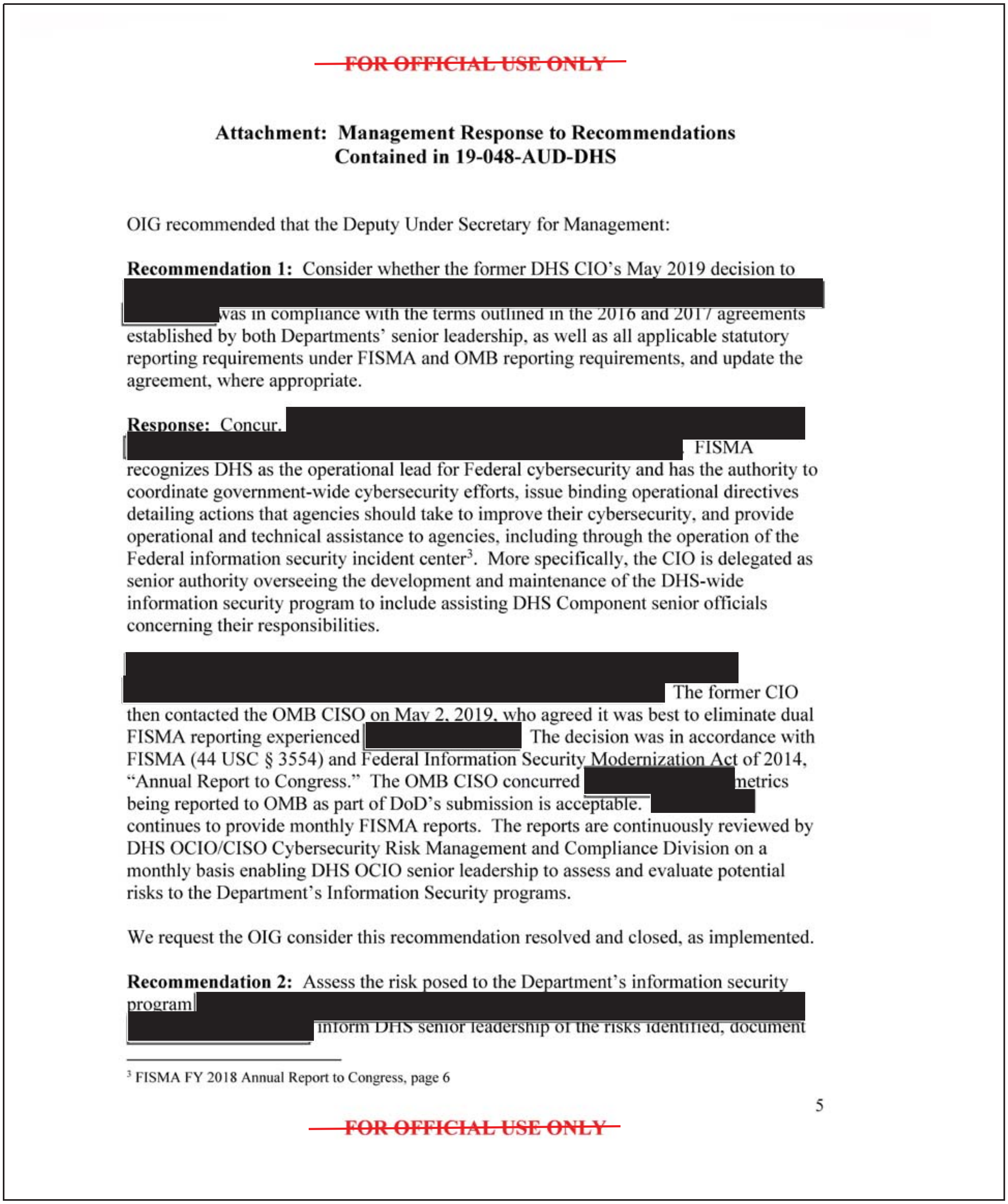
The draft report contained five recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for OIG's consideration.

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.

Attachment

4

~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~

Attachment: Management Response to Recommendations Contained in 19-048-AUD-DHS

OIG recommended that the Deputy Under Secretary for Management:

Recommendation 1: Consider whether the former DHS CIO's May 2019 decision to [redacted] was in compliance with the terms outlined in the 2016 and 2017 agreements established by both Departments' senior leadership, as well as all applicable statutory reporting requirements under FISMA and OMB reporting requirements, and update the agreement, where appropriate.

__Response:__ Concur. [redacted] FISMA recognizes DHS as the operational lead for Federal cybersecurity and has the authority to coordinate government-wide cybersecurity efforts, issue binding operational directives detailing actions that agencies should take to improve their cybersecurity, and provide operational and technical assistance to agencies, including through the operation of the Federal information security incident center[3]. More specifically, the CIO is delegated as senior authority overseeing the development and maintenance of the DHS-wide information security program to include assisting DHS Component senior officials concerning their responsibilities.

[redacted] The former CIO then contacted the OMB CISO on May 2, 2019, who agreed it was best to eliminate dual FISMA reporting experienced [redacted] The decision was in accordance with FISMA (44 USC § 3554) and Federal Information Security Modernization Act of 2014, "Annual Report to Congress." The OMB CISO concurred [redacted] metrics being reported to OMB as part of DoD's submission is acceptable. [redacted] continues to provide monthly FISMA reports. The reports are continuously reviewed by DHS OCIO/CISO Cybersecurity Risk Management and Compliance Division on a monthly basis enabling DHS OCIO senior leadership to assess and evaluate potential risks to the Department's Information Security programs.

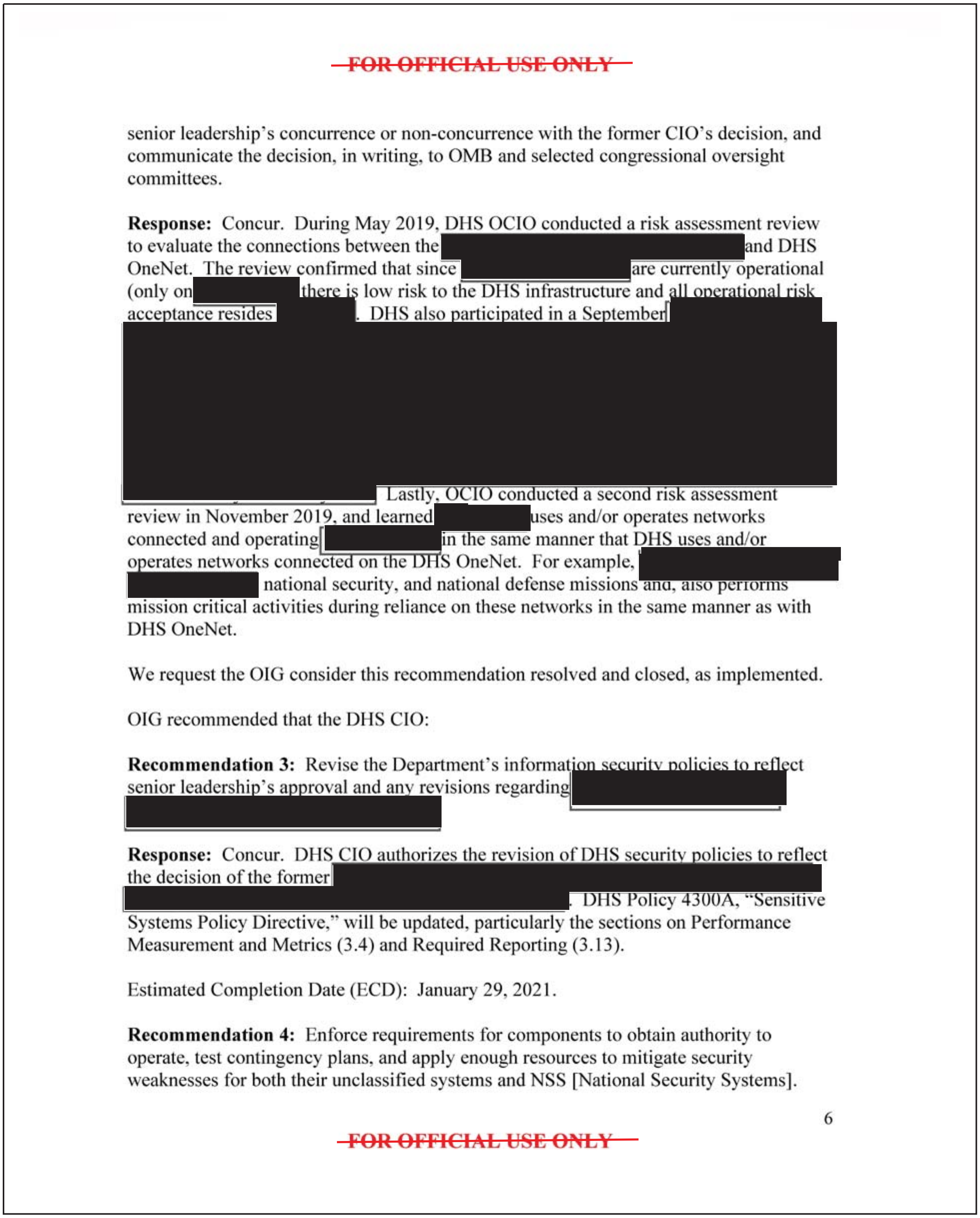
We request the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Assess the risk posed to the Department's information security program [redacted] inform DHS senior leadership of the risks identified, document

[3] FISMA FY 2018 Annual Report to Congress, page 6

5

~~FOR OFFICIAL USE ONLY~~



senior leadership's concurrence or non-concurrence with the former CIO's decision, and communicate the decision, in writing, to OMB and selected congressional oversight committees.

Response: Concur. During May 2019, DHS OCIO conducted a risk assessment review to evaluate the connections between the [redacted] and DHS OneNet. The review confirmed that since [redacted] are currently operational (only on [redacted] there is low risk to the DHS infrastructure and all operational risk acceptance resides [redacted]. DHS also participated in a September [redacted] Lastly, OCIO conducted a second risk assessment review in November 2019, and learned [redacted] uses and/or operates networks connected and operating [redacted] in the same manner that DHS uses and/or operates networks connected on the DHS OneNet. For example, [redacted] national security, and national defense missions and, also performs mission critical activities during reliance on these networks in the same manner as with DHS OneNet.

We request the OIG consider this recommendation resolved and closed, as implemented.

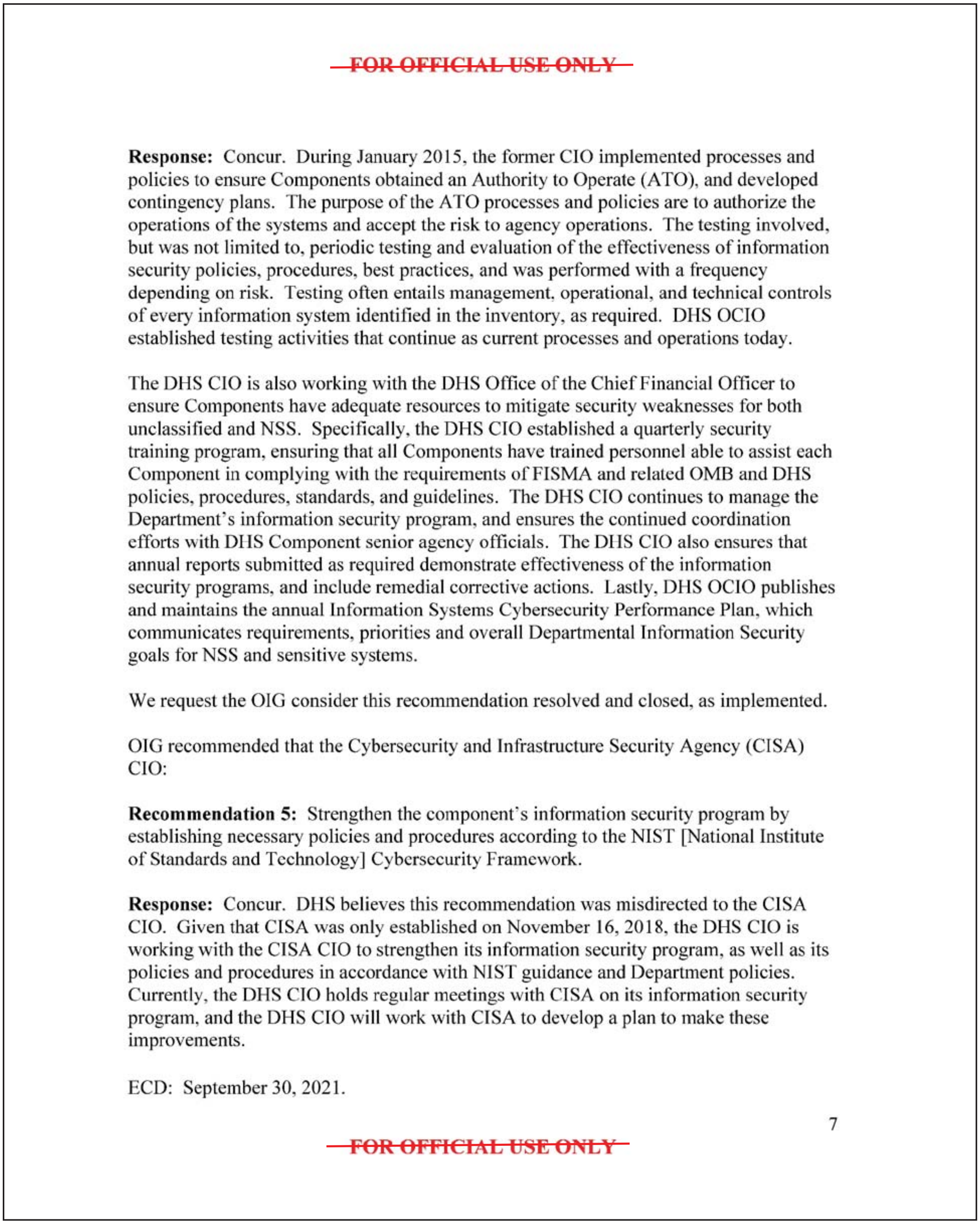
OIG recommended that the DHS CIO:

Recommendation 3: Revise the Department's information security policies to reflect senior leadership's approval and any revisions regarding [redacted]

Response: Concur. DHS CIO authorizes the revision of DHS security policies to reflect the decision of the former [redacted]. DHS Policy 4300A, "Sensitive Systems Policy Directive," will be updated, particularly the sections on Performance Measurement and Metrics (3.4) and Required Reporting (3.13).

Estimated Completion Date (ECD): January 29, 2021.

Recommendation 4: Enforce requirements for components to obtain authority to operate, test contingency plans, and apply enough resources to mitigate security weaknesses for both their unclassified systems and NSS [National Security Systems].



Response: Concur. During January 2015, the former CIO implemented processes and policies to ensure Components obtained an Authority to Operate (ATO), and developed contingency plans. The purpose of the ATO processes and policies are to authorize the operations of the systems and accept the risk to agency operations. The testing involved, but was not limited to, periodic testing and evaluation of the effectiveness of information security policies, procedures, best practices, and was performed with a frequency depending on risk. Testing often entails management, operational, and technical controls of every information system identified in the inventory, as required. DHS OCIO established testing activities that continue as current processes and operations today.

The DHS CIO is also working with the DHS Office of the Chief Financial Officer to ensure Components have adequate resources to mitigate security weaknesses for both unclassified and NSS. Specifically, the DHS CIO established a quarterly security training program, ensuring that all Components have trained personnel able to assist each Component in complying with the requirements of FISMA and related OMB and DHS policies, procedures, standards, and guidelines. The DHS CIO continues to manage the Department's information security program, and ensures the continued coordination efforts with DHS Component senior agency officials. The DHS CIO also ensures that annual reports submitted as required demonstrate effectiveness of the information security programs, and include remedial corrective actions. Lastly, DHS OCIO publishes and maintains the annual Information Systems Cybersecurity Performance Plan, which communicates requirements, priorities and overall Departmental Information Security goals for NSS and sensitive systems.

We request the OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the Cybersecurity and Infrastructure Security Agency (CISA) CIO:

Recommendation 5: Strengthen the component's information security program by establishing necessary policies and procedures according to the NIST [National Institute of Standards and Technology] Cybersecurity Framework.

Response: Concur. DHS believes this recommendation was misdirected to the CISA CIO. Given that CISA was only established on November 16, 2018, the DHS CIO is working with the CISA CIO to strengthen its information security program, as well as its policies and procedures in accordance with NIST guidance and Department policies. Currently, the DHS CIO holds regular meetings with CISA on its information security program, and the DHS CIO will work with CISA to develop a plan to make these improvements.

ECD: September 30, 2021.

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Shawn Hatch, Manager
Stefanie Holloway, IT Auditor
Thomas Rohrback, Chief, Information Assurance and Testing
James Diaz, Program Analyst
Brenden Burke, Program Analyst
Jason Dominguez, IT Specialist
Rashedul Romel, IT Specialist
Taurean McKenzie, IT Specialist
Jane DeMarines, Communications Analyst
Corneliu Buzesan, Referencer

Appendix D
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
Chief Information Officer
Chief Information Security Officer
Audit Liaison, Office of the Chief Information Officer
Audit Liaison, Office of the Chief Information Security Officer
Audit Liaisons, CBP, FEMA, ICE, I&A, USCIS, CISA, S&T, TSA, Coast Guard, and Secret Service

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