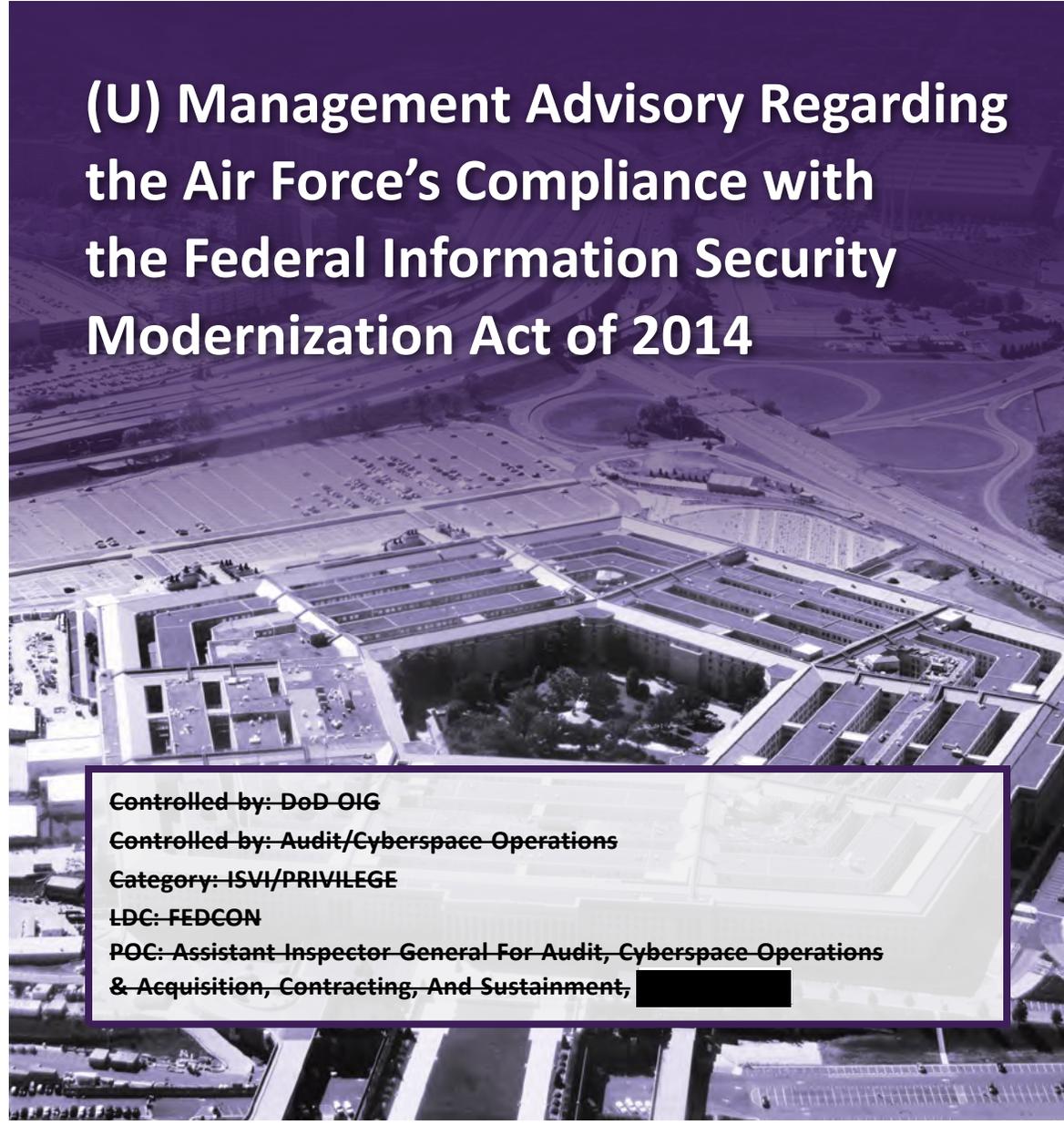


CUI

# INSPECTOR GENERAL

*U.S. Department of Defense*

OCTOBER 12, 2022



## (U) Management Advisory Regarding the Air Force's Compliance with the Federal Information Security Modernization Act of 2014

~~Controlled by: DoD-OIG~~

~~Controlled by: Audit/Cyberspace Operations~~

~~Category: ISVI/PRIVILEGE~~

~~LDC: FEDCON~~

~~POC: Assistant Inspector General For Audit, Cyberspace Operations  
& Acquisition, Contracting, And Sustainment, [REDACTED]~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

CUI





**INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500**

October 12, 2022

(U) MEMORANDUM FOR THE AIR FORCE CHIEF INFORMATION OFFICER  
AIR FORCE CHIEF PRIVACY OFFICER  
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) SUBJECT: Management Advisory Regarding the Air Force's Compliance with the  
Federal Information Security Modernization Act of 2014  
(Report No. DODIG-2023-003)

(U) The purpose of this management advisory is to provide Air Force leadership with DoD Office of Inspector General (DoD OIG) findings and recommendations specific to the Air Force's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). We identified these findings during our FY 2021 review of the DoD's compliance with FISMA, which was announced on November 18, 2020 (Project No. D2021-D000CP-0034.000). We conducted the work on this project with integrity, objectivity, and independence, as required by the Council of the Inspectors General for Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

(U) FISMA requires Federal agencies to develop, document, and implement an Agency-Wide program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA also requires Federal agency Inspectors General (IGs), or an independent external auditor designated by that IG, to conduct an annual independent review on the effectiveness of the agency's information security program and practices. IGs must submit their annual results to the Office of Management and Budget and Department of Homeland Security.

(U) For FY 2021, we assessed selected portions of the Air Force's information security program and practices as part of our annual independent review. We submitted the results of the overall effectiveness of DoD's information security program and practices to the Office of Management and Budget and Department of Homeland Security on October 28, 2021. We are issuing this management advisory to report the results specific to the Air Force and to issue recommendations for corrective action.

(U) We provided a draft copy of this management advisory to DoD management and requested written comments on the findings and recommendations. We considered management's comments on the draft when preparing the final management advisory.

(U) This management advisory contains six recommendations that we consider resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this advisory, the six recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This management advisory contains one recommendation that is considered closed as discussed in the Recommendations, Management Comments, and Our Response section of this advisory. The recommendation does not require further action.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the resolved recommendations, within 90 days please provide us documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to [followup@dodig.mil](mailto:followup@dodig.mil) if unclassified or [rfunet@dodig.smil.mil](mailto:rfunet@dodig.smil.mil) if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the review. If you have any questions, please contact me at [REDACTED]



Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations & Acquisition,  
Contracting, and Sustainment

## (U) Background

(U) On December 17, 2002, the President signed the Federal Information Security Management Act into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of the law was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. Congress amended the law on December 18, 2014, (Public Law 113-283) and renamed it the Federal Information Security Modernization Act of 2014 (FISMA). The amendment, among other things, established the Director of the Office of Management and Budget’s (OMB) authority to oversee information security policies and practices for Federal agencies and the Secretary of the Department of Homeland Security’s (DHS) authority to manage the information security policies and practices across the Federal government. FISMA requires that senior agency officials provide security for the information and information systems that support the operations and assets under their control, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

*(U) FISMA requires that senior agency officials provide security for the information and information systems that support the operations and assets under their control.*

(U) FISMA also requires that Federal agencies conduct an annual, independent review of the effectiveness of their information security program and practices. For a Federal agency with an IG appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must conduct the review and submit the results to the OMB and DHS. Each year, the OMB issues guidance that requires the IGs to assess the effectiveness their agency’s information security program using annual IG FISMA reporting metrics.<sup>1</sup> The OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency develop the IG FISMA reporting metrics, in consultation with the Federal Chief Information Officer Council.

## (U) FISMA Reporting Metrics

(U) The FY 2021 OMB guidance contained 66 IG FISMA reporting metrics.<sup>2</sup> The metrics were grouped into nine domains aligned under the five information security functions established by the National Institute of Standards and Technology (NIST) Cybersecurity Framework—

<sup>1</sup> (U) OMB Memorandum M-21-02, “Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements,” November 9, 2020.

<sup>2</sup> (U) IG FISMA metrics are questions addressing various aspects of an organization’s information security program.

*(U) The NIST Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise.*

(U) Identify, Protect, Detect, Respond, and Recover.<sup>3</sup> The NIST Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise.<sup>4</sup> Table 1 describes the nine domains by function.

*(U) Table 1. Descriptions of NIST Cybersecurity Framework Functions and FISMA Domains*

(U) Function	(U) Domain	(U) Description
(U) Identify	Risk Management	Risk management is the process of managing information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.
	Supply Chain Risk Management	Supply chain risk management is the process of ensuring that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity requirements.
(U) Protect	Configuration Management	Configuration management consists of the controls and processes for establishing and maintaining the integrity of information technology products and information systems.
	Identity and Access Management	Identity and access management consists of the controls and processes for identifying users, using credentials, and managing user access to network resources.
	Data Protection and Privacy	Data protection and privacy consists of the controls and processes for protecting systems and information (data), and ensuring management of those systems and data is consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
	Security Training	Security training consists of an established program that ensures all users complete the necessary mandatory cybersecurity training requirements before they receive access to organizational information technology resources, including specialized training for individuals requiring privileged access.
(U) Detect	Information Security Continuous Monitoring	Information security continuous monitoring is the process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
(U) Respond	Incident Response	Incident response is a formal, focused, and coordinated approach to responding to cybersecurity incidents.
(U) Recover	Contingency Planning	Contingency planning is a coordinated strategy involving plans, procedures, and technical measures that will enable the recovery of information systems, operations, and data after a disruption.

(U) Source: The DoD OIG.

<sup>3</sup> (U) “FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA),” Version 1.1, May 12, 2021. The FY 2021 IG FISMA Reporting Metrics referenced Public Law, Federal requirements, and NIST guidance as the criteria to measure the agency’s information security program and practices.

<sup>4</sup> (U) “NIST: Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, April 16, 2018. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

(U) The IGs assign a maturity level (rating) for each domain by determining whether: the agency has issued the required policies and procedures applicable to the domain; and the policies and procedures are implemented and effective. Figure 1 shows the five-level maturity model used.

(U) Figure 1. IG FISMA Maturity Model



(U) Source: FY 2021 IG FISMA Reporting Metrics.

(U) Federal agency IGs use a simple majority of the metric ratings to determine the maturity level for each domain; domain ratings are then used to determine the maturity level for each function, which IGs use to determine the overall agency rating. However, the FY 2021 IG FISMA Reporting Metrics allowed IGs to use their discretion when determining the maturity level and could adjust the rating along the scale accordingly. IGs can consider additional factors when determining the maturity levels and the agency’s overall effectiveness, such as the maturity levels for the functions and the agency’s unique missions, resources, and challenges.

## (U) Scope and Methodology

*(U) We are issuing this management advisory to report the results specific to the Air Force and to issue recommendations for corrective action.*

(U) For FY 2021, we assessed selected portions of the Air Force’s information security program and practices as part of our annual independent review of the DoD’s overall information security program and practices. We submitted the results of the overall review to the OMB and DHS on October 28, 2021, and we are issuing

this management advisory to report the results specific to the Air Force and to issue recommendations for corrective action.

(U) We conducted the Air Force assessment from November 2020 through June 2022. Specifically, we assessed whether the Air Force met the requirements outlined in the FY 2021 IG FISMA Reporting Metrics for 5 of the 66 metrics, which represented 4 of the 9 domains (see the Appendix for a list of the 5 metrics). We selected the five metrics for review using a risk-based approach that considered several factors, such as the DoD’s prior FISMA results, the impact level (high, medium, low) of each reporting metric based on related NIST guidance, and whether the DoD Office of the Chief Information Officer (CIO) tracked related information.<sup>5</sup> For each of the five metrics, we determined whether the Air Force issued policies and procedures related to the metric and whether the Air Force implemented the policies and procedures.

(U) To accomplish our review, we analyzed Air Force information technology and cybersecurity policies and procedures relevant to the five metrics and the corresponding NIST Special Publication (SP) 800-53 controls. We reviewed key documents, such as monthly status reports that officials used to track and monitor selected cybersecurity controls, plans for addressing protection of sensitive information, and other management reports supporting the Air Force’s efforts to oversee the implementation of selected metric questions. We also interviewed personnel from the Air Force CIO and the Privacy and Civil Liberties offices, which were responsible for overseeing the implementation of cybersecurity and privacy-related policies and procedures.

(U) This report was reviewed by the DoD Component associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Component about the CUI treatment of their information. If the DoD Component failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

<sup>5</sup> (U) Most FISMA metrics align with specific NIST SP 800-53 controls. Although NIST issued Revision 5 to NIST SP 800-53, “Security and Privacy Controls for Information Systems and Organizations,” September 23, 2020, agencies were not required to implement all changes until September 2021. Therefore, the FY 2021 IG FISMA metrics referenced the controls contained in Revision 4 to NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”

## (U) Air Force Roles and Responsibilities for Information Security

(U) DoD Instruction 8500.01 requires that the DoD CIO monitor, evaluate, and advise the Secretary of Defense regarding all cybersecurity activities and appoint a DoD Senior Information Security Officer to direct and coordinate the DoD cybersecurity program.<sup>6</sup> DoD Instruction 8500.01 also requires that DoD Component CIOs, on behalf of the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program that is consistent with the overall DoD cybersecurity program and appoint a DoD Component Senior Information Security Officer to coordinate their DoD Component cybersecurity program. Furthermore, Air Force guidance outlines the following roles and responsibilities pertaining to cybersecurity.<sup>7</sup>

**(U) CIO.** The Secretary of the Air Force, Office of the CIO is responsible for providing guidance and oversight to support the Air Force cybersecurity program, appointing the Air Force Chief Information Security Officer, Air Force Privacy Officer, and Authorizing Officials (AOs), and ensuring information system owners are appointed for all Air Force information technology.

**(U) Chief Information Security Officer (CISO).** The Air Force CISO is responsible for implementing and maintaining the Air Force cybersecurity program and monitoring, evaluating, and providing advice to the CIO on the Air Force cybersecurity posture.

**(U) Privacy Officer.** The Air Force Privacy Officer is responsible for implementing the Air Force privacy program and providing guidance and assistance to Air Force privacy managers.

**(U) Major Command (MAJCOM) Cybersecurity Office.** The MAJCOM Cybersecurity Office is responsible for supporting the CISO's cybersecurity program for the MAJCOM's bases to include ensuring that the cybersecurity workforce is qualified and requirements are tracked.<sup>8</sup>

**(U) Authorizing Official.** AOs are the only officials with the authority to grant authorization decisions for information technology systems. AOs grant an authorization after determining whether the overall risks of operating a system are at acceptable level to support mission requirements.

<sup>6</sup> (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, (Incorporating Change 1, October 7, 2019).

<sup>7</sup> (U) Air Force Instruction 17-101, "Risk Management Framework (RMF) For Air Force Information Technology (IT)," February 6, 2020.  
(U) Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," March 10, 2020.  
(U) Air Force Instruction 17-130, "Cybersecurity Program Management," February 13, 2020.

<sup>8</sup> (U) A MAJCOM represents a major command assigned responsibility of a specific portion of the Air Force mission. The Air Force has nine MAJCOMs that report directly to the Air Force Headquarters. The Air Force MAJCOMs are organized by mission, such as the Air Combat or Mobility Commands, or by region, such as the Europe or Pacific Air Forces.

**(U) Information System Owner.** Information system owners are responsible for the overall procurement, development, integration, modification, and operation and maintenance of Air Force information technology systems and are responsible for performing Program Manager (PM) duties when a PM is not assigned.

**(U) Program Manager.** PMs are responsible for ensuring that operational information technology systems maintain an authorization to operate (ATO) and for recommending to the AO that systems without an ATO be removed from the network. PMs also are responsible for managing corrective actions identified in any plan of action and milestones (POA&M) for their assigned systems.<sup>9</sup>

**(U) Information System Security Manager.** The Information System Security Manager is the primary cybersecurity technical advisor to the AO, PM, and information system owner. The Information System Security Manager also supports the Information System Owner in maintaining ATOs and implementing corrective actions identified in POA&Ms.

**(U) Information System Security Officer.** The Information System Security Officer is responsible for ensuring the appropriate operational security posture is maintained to protect information technology systems.

## (U) Air Force Information Security Program and Practices

*(U) Although the Air Force had policies and procedures in place for the five metrics we reviewed, it did not consistently implement the policies and procedures for four of the five metrics.*

(U) Although the Air Force had policies and procedures in place for the five metrics we reviewed, it did not consistently implement the policies and procedures for four of the five metrics. Specifically, Air Force officials tracked user completion of annual cybersecurity awareness training (Metric 44); however, for the remaining four metrics, Air Force officials did not:

- (U) track and monitor the mitigation of system security weaknesses identified in POA&Ms within established timeframes (Metric 8);<sup>10</sup>
- (U) report privacy related breaches within established timeframes (Metric 38);
- (U) ensure that privacy awareness training addressed all key elements required by Air Force guidance (Metric 39); and
- (U) ensure that all systems had an ATO as required to be on the Air Force network (Metric 49).

<sup>9</sup> (U) A POA&M is a document used to record the known weaknesses (risks) in a system or network, the actions and resources needed to mitigate those weaknesses, and the expected milestones and completion dates for mitigating the weaknesses.

<sup>10</sup> (U) FISMA, NIST, and the Air Force use the terms weakness and vulnerability interchangeably, but we primarily use the term weakness for purposes of this advisory.

(U) Consistent implementation of cybersecurity policies and procedures is critical for an effective cybersecurity program and reduces the risk of successful cyber attacks, data breaches, data loss and manipulation, or unauthorized disclosures of mission-essential or sensitive information by malicious actors. Therefore, the Air Force should take action to address the recommendations in this management advisory, which will result in more consistent implementation of the policies and procedures associated with the four metrics we reviewed and reduce the associated risk.

## (U) Identify Function/Risk Management Domain

(U) For the identify function/risk management domain we assessed FY 2021 IG FISMA Reporting Metric 8, which asks, *“To what extent has the organization ensured that POA&Ms are utilized for effectively mitigating security weaknesses?”*

(U) The Air Force had policies and procedures in place that required the use of POA&Ms for mitigating security weaknesses, and developed POA&Ms when it identified weaknesses. However, the Air Force system owners were not monitoring and tracking the POA&Ms to ensure that the weaknesses were mitigated in accordance with Air Force policies and procedures. NIST SP 800-53 requires that organizations prepare POA&Ms to document planned mitigation or remediation steps to correct weaknesses identified and to reduce or eliminate known weaknesses. Air Force Instruction 17-101 aligns with NIST SP 800-53 and requires that information system owners prepare POA&Ms when system weaknesses are identified and document the progress in mitigating the weaknesses on the POA&M.<sup>11</sup> The Air Force POA&M Guidebook states that PMs or Information System Security Managers are responsible for implementing the corrective actions identified in POA&Ms. The Guidebook also states that the CIO and AOs are responsible for monitoring and tracking the overall execution of system-level POA&Ms until closure of the identified weaknesses. Further, the Guidebook requires correction of all very high and high weaknesses within 30 days and mitigation of all moderate weaknesses within 90 days. A very high weakness is exposed and exploitable, and its exploitation could result in severe operational impact; relevant security controls are not planned or are not identified. A high weakness is based on the exposure of the weakness, ease of exploitation, and the severity of the impact; relevant security controls are planned but not implemented or compensating controls are in place and minimally effective. A moderate weakness is based on the exposure of the weakness, ease of exploitation and severity of the impact; relevant security controls are planned, partially implemented, and somewhat effective.

*:(U) The Air Force system owners were not monitoring and tracking the POA&Ms to ensure that the weaknesses were mitigated in accordance with Air Force policies and procedures.*

<sup>11</sup> (U) Air Force Instruction 17-101, “Risk Management Framework (RMF) for Air Force Information Technology (IT),” February 6, 2020.

~~(CUI)~~ Although the Air Force information system owners were preparing POA&Ms to address known weaknesses, Air Force CIO officials were not always monitoring and tracking the status of the very high, high, and moderate weaknesses to ensure that system owners mitigated identified weaknesses within establish timeframes. The Air Force tracks its POA&Ms in the Enterprise Mission Assurance Support Service (eMASS). eMASS is a web-based tool used to capture key system information such as system security plans, security-control test results, POA&Ms, and authorization decisions (granting ATOs). On August 30, 2021, the Air Force alternate Senior Information System Officer provided a report identifying that the Air Force had [REDACTED] [REDACTED] moderate weaknesses recorded in eMASS. Although the eMASS report did not age the weaknesses by their development date, it indicated that all [REDACTED] very high, high, and moderate weaknesses were at least 120 days past their scheduled completion date; and therefore, past the 30-day and 90-day mitigation requirements respectively.

~~(CUI)~~ Additionally, we reviewed the [REDACTED] very high or high weakness from the Air Force's eMASS POA&M report to determine whether any weaknesses were included in the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities (weaknesses) catalog.<sup>12</sup> We determined that [REDACTED] of the high weaknesses were associated with weaknesses in the known exploited vulnerabilities catalog, which could allow malicious actors to bypass user authentication and perform unauthorized activity on information systems resulting in system compromise. The Cybersecurity and Infrastructure Security Agency requires that Federal agencies remediate weaknesses in the catalog by implementing the identified corrective actions or by removing the affected system from their network.

(U) By having unmitigated and actively exploited weaknesses on their systems, officials increased the risk of successful cyber attacks, system and data breaches, data loss and manipulation, or unauthorized disclosures of mission-essential or sensitive information by malicious actors to the Air Force network. Therefore, we recommend that the Air Force CIO direct the systems owners, in coordination with the Air Force CISO and the AOs, to identify and mitigate all very high, high, and moderate weaknesses identified in POA&Ms that exceed the 30-day and 90-day mitigation requirement as required by Air Force guidance, and prioritize any weaknesses identified in the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities catalog (Recommendation 1.a). We also recommend that the Air Force CIO establish controls, in coordination with the Air Force CISO and AOs, to ensure that system owners mitigated weaknesses identified in POA&Ms by their scheduled completion dates and in accordance with the timelines established in Air Force guidance (Recommendation 1.b).

<sup>12</sup> (U) The Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security, is responsible for managing a catalog of known exploited vulnerabilities that carry significant risk to the Federal government. An active exploitation occurs when there is evidence that malicious actors are actively exploiting known system vulnerabilities without knowledge of the system owners.

(U) NIST SP 800-53 defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

## (U) Protect Function/Data Protection and Privacy Domain

(U) For the Protect Function/Data Protection and Privacy Domain we assessed two FY 2021 IG FISMA Reporting Metrics:

- (U) Metric 38, which asks, “*To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?*”<sup>13</sup>
- (U) Metric 39, which asks, “*To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?*”

### (U) Data Breach Response Plan

(U) The Air Force implemented the October 2017 DoD Breach Response Plan, and had additional policies and procedures in place for responding to privacy-related breaches.<sup>14</sup> However, Air Force officials did not always report privacy-related breaches within required timeframes. A breach is a privacy incident that results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or an authorized user accesses PII for an other-than-authorized purpose.<sup>15</sup> A privacy incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the PII the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. NIST SP 800-53 requires that organizations develop and implement a response plan for privacy incidents, and provide a response to privacy incidents in accordance with the organizational response plan for privacy incidents.

⋮ (U) Air Force officials  
 ⋮ did not always report  
 ⋮ privacy-related breaches  
 ⋮ within required timeframes.

(U) The October 2017 DoD Breach Response Plan aligns with NIST SP 800-53 and provides the DoD with procedures for preparing for and responding to known or suspected privacy related breaches. Air Force Instruction 33-332 is the Air Force’s implementing guidance that aligns with the DoD Breach Response Plan and requires the Air Force Privacy Officer to issue guidance and procedures to ensure the protection of PII and to provide guidance and assistance to MAJCOM privacy managers. The Instruction also requires the Air Force Privacy Officer to submit a privacy-related breach report (DD Form 2959) to Chief of the DoD’s Privacy, Civil Liberties, and Freedom of Information Division (PCLFD) through the compliance and reporting tool within 48 hours of a breach notification.

<sup>13</sup> (U) A privacy event is any observable occurrence in a system or network that may indicate that a privacy incident is occurring.

<sup>14</sup> (U) Office of the Deputy Chief Management Officer, “DoD Breach Response Plan,” October 31, 2017. In November 2018, the Deputy Secretary of Defense issued a memorandum, “Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan,” to supplement the October 2017 DoD Breach Response Plan.

(U) Effective October 1, 2021, the Deputy Secretary of Defense disestablished the Chief Management Officer and transferred, among other things, oversight and privacy and data breach responsibilities to the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

<sup>15</sup> (U) PII is information that can be used to distinguish or trace an individual’s identity.

(U) However, Air Force privacy officials did not always report privacy-related breaches in accordance with the required timeframes. As of July 2021, the Air Force had not reported any major privacy-related breaches in FY 2021, but did report 159 confirmed minor breaches to the PCLFD.<sup>16</sup> We nonstatistically selected 19 of the 159 confirmed minor privacy-related breaches to review. Of the 19 minor privacy-related breaches reviewed, we determined that Air Force officials did not report 16 breaches to the PCLFD within 48 hours. For one of the reported events, the Air Force Privacy Officer took over 4 months to report the breach to the PCLFD. These minor privacy related breaches involved instances in which unsecure documents containing PII were e-mailed or stored on shared drives or servers.

(U) Delayed reporting of privacy-related breaches limits the Air Force’s ability to reduce the potential harm caused by unauthorized access to PII and other sensitive data; thus, Air Force privacy officials need to ensure that personnel are reporting breaches to the appropriate officials within a timely manner. Therefore, we recommend that the Air Force Privacy Officer establish controls to ensure that privacy officials are timely reporting breaches in accordance with Air Force Instruction 33-332 (Recommendation 2.a).

***(U) Updated DoD Data Breach Plan***

(U) In May 2021, the DoD issued a revised Data Breach Response Plan for DoD Components to use and implement within their subcomponents.<sup>17</sup> The revised plan included changes to the privacy-related breach reporting process. For example, the updated plan requires that Component Privacy Officers report breaches to the DoD Component security operation center, which in turn reports the breaches through its chain of command to the U.S. Cyber Command. The U.S. Cyber Command is responsible for reporting the privacy related breaches to the U.S. Computer Emergency Readiness Team, which

*(U) Air Force officials had not updated the Air Force Instruction 33-332 to align with the revisions from the June 2021 DoD Data Breach Response Plan.*

is part of the Department of Homeland Security. The U.S. Computer Emergency Readiness Team is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. However, Air Force

officials had not updated the Air Force Instruction 33-332 to align with the revisions from the June 2021 DoD Data Breach Response Plan. Therefore, we recommend that the Air Force CIO update Air Force Instruction 33-332, in coordination with the Air Force Privacy Officer, to align with the June 2021 DoD Data Breach Response Plan, including the changes to the breach reporting process (Recommendation 1.c).

<sup>16</sup> (U) A major breach is an incident that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. Minor breaches are those that do not meet the definition of a major breach.

<sup>17</sup> (U) DoD Manual 5400.11, Volume 2, “DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan,” May 6, 2021.

### **(U) Privacy Training**

(U) The Air Force had policies and procedures in place that required its personnel (military members, civilians, and contractors) to take privacy awareness training annually, including role-based training. However, the Air Force privacy officials did not provide annual privacy training that included all content required by

Air Force Instruction 33-332. NIST SP 800-53 directs organizations to oversee basic privacy training and targeted, role-based privacy training at least annually and, where appropriate, organizations may provide privacy training as part of existing information security training. Air Force Instruction 33-332 aligns with the

*(U) The Air Force privacy officials did not provide annual privacy training that included all content required by Air Force Instruction 33-332.*

NIST SP 800-53 requirements and states that Air Force MAJCOMs and Wing Commanders should ensure that all assigned personnel complete annual privacy training, such as awareness training, focusing on individual’s roles and responsibilities of the Privacy Act and safeguarding PII.

(U) According to the Privacy and Civil Liberties Officer, the Air Force uses the DoD Cyber Awareness Challenge course to provide annual privacy awareness training to its personnel. Although the primary focus of the course is cybersecurity, it also addresses how to identify and safeguard PII. The course is mandatory and is required annually for all users that have access to Air Force information systems.<sup>18</sup> However, the DoD Cyber Awareness Challenge course does not address all privacy awareness training elements or Privacy Act responsibilities outlined in Air Force Instruction 33-332, such as the collection, maintenance, and use of privacy information to support programs that are authorized by law or executive order and are implemented by DoD and Air Force guidance.

(U) Privacy training helps to increase personnel awareness of PII, how PII should be protected, and the privacy requirements that reduce the risk of noncompliance with the Privacy Act. Failure to adequately safeguard PII can also increase the risk of potential breaches and loss of PII. Therefore, we recommend that the Air Force Chief Privacy Officer ensure that all Air Force personnel receive annual privacy awareness training that addresses all the key elements required by Air Force Instruction 33-332 (Recommendation 2.b).

### **(U) Protect Function/Security Training Domain**

(U) For the Protect Function/Security Training Domain we assessed FY 2021 IG FISMA Reporting Metric 44, which asks, “*To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems?*”

<sup>18</sup> (U) See discussion in Metric 44 on how the Air Force tracks completion of privacy training.

(U) The Air Force had policies and procedures in place that required all network users to complete security awareness training annually, and ensured that the training was tailored based on mission, risk environment, and types of information systems as required. The Air Force officials established a process to track that users (military members, civilians, and contractors) completed the annual security awareness training in a timely manner.

*(U) The Air Force officials established a process to track that users (military members, civilians, and contractors) completed the annual security awareness training in a timely manner.*

(U) NIST SP 800-53 directs organizations to provide basic security awareness training to information system users as part of initial training, when required by system changes, and at an organizationally defined frequency thereafter. Air Force Manual 17-1303 aligns with the NIST SP 800-53 requirement and states that all network

users must complete initial and annual cybersecurity awareness training as a condition of access to the network.<sup>19</sup> The Air Force uses the DoD Cyber Awareness Challenge course to meet the initial and annual required cybersecurity awareness training, which includes instruction on cybersecurity requirements in key areas such as e-mail, mobile devices, social media, phishing, malware, and physical security and provides DoD users with actions they should take to defend against the associated risks.

(U) Air Force Manual 17-1303 requires that Air Force officials document and maintain the status of user awareness training. Air Force officials explained that new employees must complete initial cybersecurity awareness training as part of the onboarding process. Air Force officials further explained that they use a learning management system to track whether Air Force network users have completed annual cybersecurity awareness training. The system tracks the status of cybersecurity awareness training, and if a user does not take the training by their annual date, the system places the user into a “quarantine status” beginning the next day. The quarantine status does not allow the user to access the Air Force network. Once the user completes cybersecurity awareness training, Air Force officials stated that the user is removed from quarantine status and can access the Air Force network.

(U) Because the Air Force has policies and procedures pertaining to security awareness training and ensured that the policies and procedures were consistently implemented to ensure that users completed annual security awareness training, we are not making a recommendation for this metric.

<sup>19</sup> (U) Air Force Manual 17-1303, “Air Force Cybersecurity Workforce Improvement Program,” May 12, 2020. The awareness training is a DoD course updated annually by the DoD CIO to remain current with the DoD information system environment.

## (U) Detect Function/Information Security Continuous Monitoring Domain

(U) For the Detect Function/Information Security Continuous Monitoring Domain we assessed FY 2021 IG FISMA Reporting Metric 49, which asks, “How mature are the organization’s processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?”

~~(CUI)~~ The Air Force had policies and procedures in place that require information system owners to conduct system assessments, obtain system authorizations, develop and maintain system security plans, and monitor security controls. However, Air Force system owners did not ensure that all systems had an ATO as required to be on the Air Force network. Specifically, we identified that approximately [redacted] of the unclassified Air Force systems were operating without a valid ATO as of September 29, 2021.

~~(CUI)~~ We identified that approximately [redacted] of the unclassified Air Force systems were operating without a valid ATO as of September 29, 2021.

(U) NIST SP 800-53 requires that organizations assess the security controls for information systems and its operational environment to determine the extent to which the controls are implemented correctly, and produces a security assessment report that documents the results of the assessment. Air Force Instruction 17-101 aligns with NIST SP 800-53 and requires privacy and security controls to be implemented based on the assessed and mitigated residual risk. Air Force Instruction 17-101 also requires controls to be aligned with DoD Instruction 8510.01 and documented in the DoD Risk Management Framework (RMF) security authorization package or ATO.<sup>20</sup> The Air Force implements the DoD RMF process and uses eMASS to document the cybersecurity risk management and system authorization process. Air Force AOs grant ATOs after they have verified that the overall system risk is at an acceptable level for mission requirements and the network.

~~(CUI)~~ Despite having DoD and Air Force guidance and procedures in place for performing ongoing security control assessments and granting ATOs, Air Force CIO officials reported that [redacted] unclassified systems were operating without a valid ATO, as of September 29, 2021. To address this issue, Air Force officials stated that they developed an unofficial “get-well” plan to reduce the number of systems without an ATO, with the goal of having all of their unauthorized systems approved by mid-April 2022. However, as of June 2022, Air Force officials stated that they still have [redacted] systems without a valid ATO as required by DoD and Air Force guidance.

<sup>20</sup> (U) DoD Instruction 8510.01 outlines the DoD RMF process and provides procedural guidance for the acceptance of authorization decisions within DoD for the authorization and connection of information systems (granting ATOs). The DoD RMF process is a step-by-step, risk-based approach to identify the security controls needed to protect systems, networks, and data consisting of six steps throughout the information system’s life cycle: 1) categorize the system, 2) select security controls, 3) implement security controls, 4) assess security controls, 5) authorize the system, and 6) monitor security controls.

(U) By having systems without a valid ATO, the Air Force CIO has no assurance that system owners implemented the necessary privacy and security controls to mitigate known weaknesses for the unauthorized information systems, which increases the risk of successful cyber attacks and the exploitation of cybersecurity system weaknesses. Therefore, we recommend that the Air Force CIO direct AOs, in coordination with the Air Force CISO, to ensure that the remaining unclassified systems have a valid ATO in accordance with DoD and Air Force guidance (Recommendation 1.d). We also recommend that the Air Force CIO establish controls, in coordination with the Air Force CISO and AOs, to ensure that the information system owners obtain and maintain ATOs for their systems as required by DoD and Air Force guidance and before placing them on the Air Force network (Recommendation 1.e).

## **(U) Recommendations, Management Comments, and Our Response**

### **(U) Recommendation 1**

(U) We recommend that the Air Force Chief Information Officer:

- a. **(U) Direct the system owners, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to identify and mitigate all very high, high, and moderate weaknesses identified in plans of action and milestones that exceed the 30-day and 90-day mitigation requirement as required by Air Force guidance, and prioritize any weaknesses identified in the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities catalog.**

### **(U) Department of Air Force Comments**

(U) The Air Force Deputy CIO, responding for the CIO, agreed, stating that the Air Force CISO will update the POA&M Guidebook to ensure that system owners remediate all very high, high, and moderate weaknesses that exceed the 30-day and 90-day mitigation requirement as required by Air Force guidance, and prioritize any weaknesses identified in the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities catalog. The Deputy CIO noted that the Air Force plans to update the guidance by March 30, 2023.

### **(U) Our Response**

(U) Comments from the Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation demonstrating that the CISO updated the POA&M Guidebook to require that system owners remediate weaknesses that exceed established timeframes as required by Air Force guidance, prioritizing the weaknesses in the known exploited vulnerabilities catalog.

- b. (U) Establish controls, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to ensure that system owners mitigated weaknesses identified in plan of action and milestones by their scheduled completion dates and in accordance with the timelines established in Air Force guidance.**

***(U) Department of Air Force Comments***

(U) The Air Force Deputy CIO, responding for the CIO, agreed, stating that the Air Force CISO will update the Air Force Organizational Risk Tolerance Baseline to include the POA&M controls used by AOs to ensure that system owners mitigate weaknesses in accordance with the timelines established in Air Force guidance. The Deputy CIO noted that the Air Force plans to update the guidance by March 30, 2023.

***(U) Our Response***

(U) Comments from the Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation demonstrating that the CISO updated the Air Force Organizational Risk Tolerance Baseline to provide the necessary POA&M controls for AOs.

- c. (U) Update Air Force Instruction 33-332, “Air Force Privacy and Civil Liberties Program,” March 10, 2020 (updated on May 12, 2020), in coordination with the Air Force Privacy Officer, to align with the June 2021 DoD Data Breach Response Plan, including the changes to the breach reporting process.**

***(U) Department of Air Force Comments***

(U) The Air Force Deputy CIO, responding for the CIO, agreed, stating that the Air Force Privacy Office will update Air Force Instruction 33-332 to align with the June 2021 DoD Data Breach Response Plan. The Deputy CIO said that the Air Force Privacy Office will update the guidance by March 30, 2023.

***(U) Our Response***

(U) Comments from the Air Force Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation demonstrating that the Air Force Privacy Office updated Air Force Instruction 33-332 to align with the current DoD Data Breach Response Plan.

- d. **(U) Direct Authorizing Officials, in coordination with the Air Force Chief Information Security Officer, to ensure that the remaining unclassified systems have a valid authorization to operate in accordance with DoD and Air Force guidance.**

***(U) Department of Air Force Comments***

~~(CUI)~~ The Air Force Deputy CIO, responding for the CIO, agreed, stating that the Air Force CISO established a process to direct AOs to ensure that unclassified systems have a valid ATO in accordance with DoD and Air Force guidance. The Deputy CIO stated that the Air Force's authorization percentage for unclassified systems was █████ percent according to the September 6, 2022 eMASS report.

***(U) Our Response***

(U) Comments from the Air Force Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation demonstrating that the remaining unclassified systems have a valid ATO.

- e. **(U) Establish controls, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to ensure that the information system owners obtain and maintain authorizations to operate for their systems as required by DoD and Air Force guidance and prior to placing them on the Air Force network.**

***(U) Department of Air Force Comments***

(U) The Air Force Deputy CIO, responding for the CIO, agreed, stating that the Air Force CISO established controls to ensure that the information system owners obtain and maintain an ATO for their systems before placing them on the Air Force network as required by DoD and Air Force guidance. In addition, the Deputy CIO said that the Air Force CISO issued a guidance memorandum to Air Force Instruction 17-101 in June 2022, which updated the Organizational Risk Tolerance Baseline to allow incremental ATOs for all Air Force systems.

***(U) Our Response***

(U) Comments from the Deputy CIO addressed the specifics of the recommendation. We verified that the Air Force CISO issued a guidance memorandum to Air Force Instruction 17-101, which outlines the Air Force's updated process for obtaining an ATO before placing an information system on the Air Force network while implementing an incremental ATO approach. We also considered the Deputy CIO's response to Recommendation 1.d and the actions taken to establish a process to ensure that all unclassified systems have a valid ATO. Therefore, the recommendation is closed, and no further comments are required.

## ***(U) Recommendation 2***

**(U) We recommend that the Air Force Chief Privacy Officer:**

- a. **(U) Establish controls to ensure that Air Force privacy officials are timely reporting breaches in accordance with the Air Force Instruction 33-332, “Air Force Privacy and Civil Liberties Program,” March 10, 2020 (updated on May 12, 2020).**

### ***(U) Department of Air Force Comments***

(U) The Air Force Deputy CIO, responding for the Air Force Chief Privacy Officer, agreed, stating that the Air Force Privacy Office will ensure additional controls are established as part of the update to Air Force Instruction 33-332 as mentioned in the response to Recommendation 1.c. The Deputy CIO noted that the Air Force Privacy Office will update the guidance by March 30, 2023.

### ***(U) Our Response***

(U) Comments from the Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation verifying that the Air Force Privacy Office updated Air Force Instruction 33-332 to include additional controls for reporting breaches in a timely manner.

- b. **(U) Ensure that all Air Force personnel receive annual privacy training that addresses all the key elements required by Air Force Instruction 33-332, “Air Force Privacy and Civil Liberties Program,” March 10, 2020 (updated on May 12, 2020).**

### ***(U) Department of Air Force Comments***

(U) The Air Force Deputy CIO, responding for the Air Force Chief Privacy Officer, agreed, stating that the Air Force CISO, in coordination with the cyber workforce training management office, will coordinate with the Defense Information Systems Agency to review the annual Cyberawareness Challenge training to identify gaps and update the course to address all the key elements required by Air Force Instruction 33-332. The Deputy CIO noted that the CISO plans to complete these actions by June 30, 2023.

### ***(U) Our Response***

(U) Comments from the Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Air Force CIO provides documentation verifying that all Air Force personnel receive privacy training that addresses all key elements required by Air Force Instruction 33-332.

## (U) Appendix

### (U) IG FISMA Reporting Metrics Reviewed at the Air Force

(U) FISMA Function (Domain)	(U) Metric No.	(U) Metric Question
(U) Identify (Risk Management)	8	To what extent has the organization ensured that POA&Ms are utilized for effectively mitigating security weaknesses?
(U) Protect (Data Protection and Privacy)	38	To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?
(U) Protect (Data Protection and Privacy)	39	To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?
(U) Protect (Security Training)	44	To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: Awareness-training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?)
(U) Detect (Information Security Continuous Monitoring)	49	How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?

(U) Source: The DoD OIG.

# (U) Management Comments

## (U) Department of Air Force



DEPARTMENT OF THE AIR FORCE  
WASHINGTON DC

21 September 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN  
1800 Air Force Pentagon Suite 4E226  
Washington, DC 20330

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Management Advisory Regarding the Air Force's Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2021-D000CP-0034.001)

1. This is the Department of the Air Force response to the DoDIG Draft Management Advisory Regarding the Air Force's Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2021-D000CP-0034.001).
2. The Department of the Air Force Chief Information Officer generally concurs with the report and welcomes the opportunity to provide a response. The Chief Information Officer, in coordination with the MAJCOMs, will correct issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendations:

**RECOMMENDATION 1.** We recommend that the Air Force Chief Information Officer:

- a. Direct the systems owners, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to identify and mitigate all very high, high, and moderate weaknesses identified in plans of action and milestones that exceed the 30-day and 90-day mitigation requirement as required by Air Force guidance, and prioritize any weaknesses identified on the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities catalog.
- b. Establish controls, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to ensure that system owners mitigated weaknesses identified in plan of action and milestones by their scheduled completion dates and in accordance with the timelines established in Air Force guidance.
- c. Update Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," March 10, 2020 (updated on May 12, 2020), in coordination with the Air Force Privacy Officer, to align with the June 2021 DoD Data Breach Response Plan, including the changes to the breach reporting process.
- d. Direct Authorizing Officials, in coordination with the Air Force Chief Information Security Officer, to ensure that the remaining unclassified systems have a valid authorization to operate in accordance with DoD and Air Force guidance.
- e. Establish controls, in coordination with the Air Force Chief Information Security Officer and Authorizing Officials, to ensure that the information system owners

## (U) Department of Air Force (cont'd)

obtain and maintain authorizations to operate for their systems as required by DoD and Air Force guidance and prior to placing them on the Air Force network.

**AIR FORCE RESPONSE:** The Air Force concurs with the intent of the recommendations listed above. The specific actions to be taken and current status are:

- a. The Air Force Chief Information Security Officer will update the Plans of Action and Milestones Guidebook to ensure system owners remediate all very high, high, and moderate weaknesses that exceed the 30-day and 90-day mitigation requirement as required by Air Force guidance, and prioritize any weaknesses identified on the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities catalog. **Estimated Completion Date: 30 March 2023.**
- b. The Air Force Chief Information Security Officer will update the DAF Organizational Risk Tolerance Baseline (ORTB) to include the CA-5 | Plan of Action and Milestones and CA-5(1) | Plan of Action and Milestones | Automation Support for Accuracy / Currency controls used by Authorizing Officials to ensure that system owners mitigate weaknesses in accordance with the timelines established in Air Force guidance. **Estimated Completion Date: 30 March 2023.**
- c. The Air Force Privacy Office will update Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," March 10, 2020 (updated on May 12, 2020) to align with the June 2021 DoD Data Breach Response Plan. **Estimated Completion Date: 30 March 2023.**
- d. The Air Force Chief Information Security Officer has established a process to direct Authorizing Officials to ensure unclassified systems have a valid authorization to operate in accordance with DoD and Air Force guidance. As of 6 September 2022 the current authorization percentage for unclassified systems is [REDACTED] per the eMASS Cybersecurity Scorecard Dashboard Report. **Request that this recommendation be CLOSED.**
- e. The Air Force Chief Information Security Officer has established controls, in coordination with Authorizing Officials, to ensure that the information system owners obtain and maintain authorizations to operate for their systems as required by DoD and Air Force guidance and prior to placing them on the Air Force network. In June 2022, the DAF CISO published a memorandum (DAFGM) to AFI 17-101 to update the ORTB to provide for incremental ATO delivery for all DAF systems. **Request that this recommendation be CLOSED.**

**RECOMMENDATION 2.** We recommend that the Air Force Chief Privacy Officer:

- a. Establish controls to ensure that Air Force privacy officials are timely reporting breaches in accordance with the Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," March 10, 2020 (updated on May 12, 2020).
- b. Ensure that all Air Force personnel receives annual privacy awareness training that addresses all the key elements required by Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," March 10, 2020 (updated on May 12, 2020).

## (U) Department of Air Force (cont'd)

**AIR FORCE RESPONSE:** The Air Force concurs with the intent of the recommendations listed above. The specific actions to be taken are:

- a. The Air Force Privacy Office will ensure additional controls are established as part of the update to Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program," described in the response to Recommendation 1c. above. **Estimated Completion Date: 30 March 2023.**
- b. The Air Force Chief Information Security Officer, in coordination with the cyber workforce training management office, will coordinate with DISA to review the annual Cyberawareness Challenge training to identify gaps and update the course to address all the key elements required by Air Force Instruction 33-332, "Air Force Privacy and Civil Liberties Program". **Estimated Completion Date: 30 June 2023.**

3. The Air Force Point of Contact [REDACTED]

BEAUCHAMP.WINS [REDACTED]  
TON.A. [REDACTED]

WINSTON A. BEAUCHAMP, SES, DAF  
Deputy Chief Information Officer



## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto:Whistleblowerprotectioncoordinator@dodig.mil)*

## **For more information about DoD OIG reports or activities, please contact us:**

### **Congressional Liaison**

703.604.8324

### **Media Contact**

[public.affairs@dodig.mil](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

### **Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

**CUI**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

**CUI**