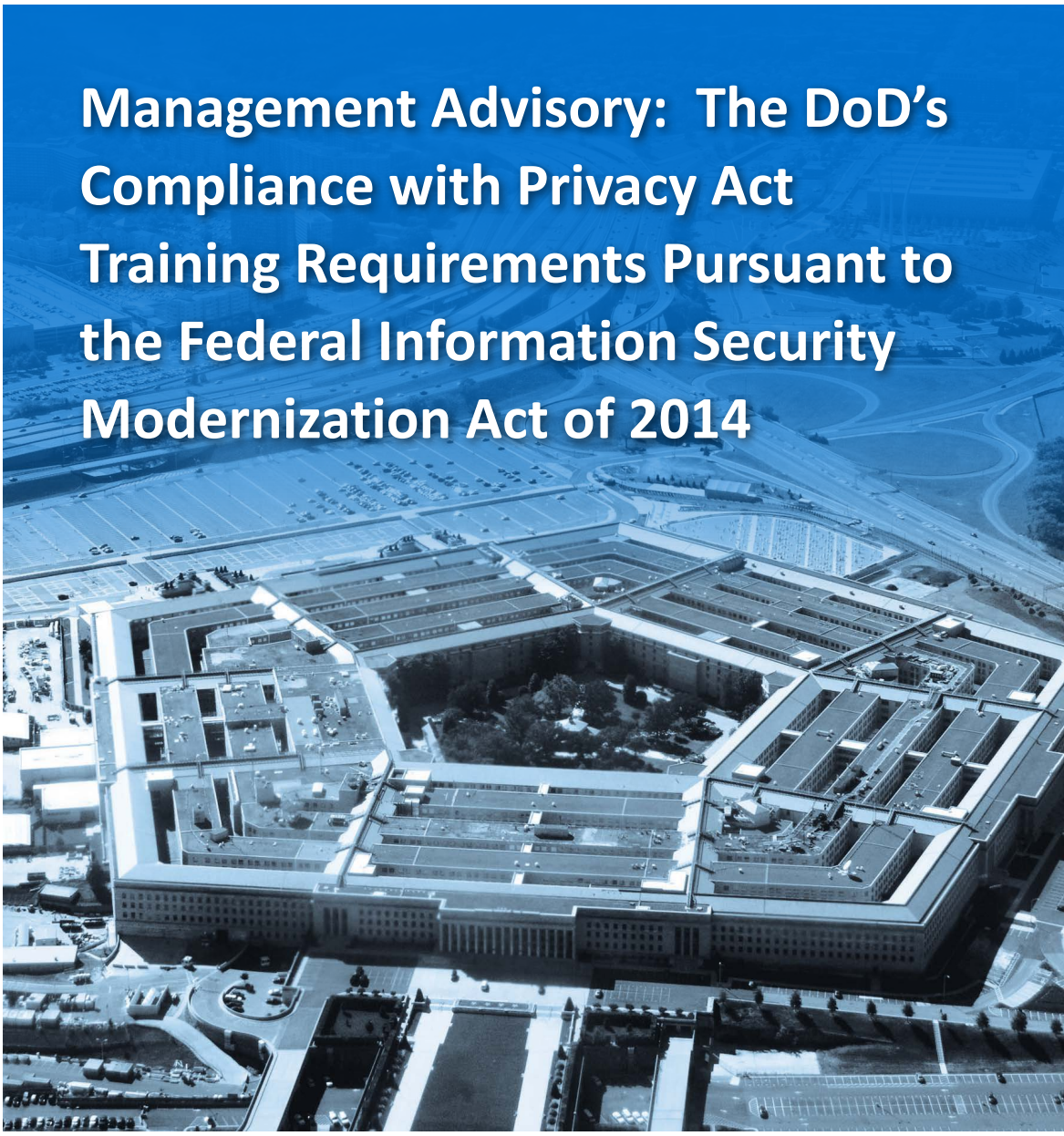
Report No. DODIG-2023-033

INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 30, 2022

Management Advisory: The DoD's Compliance with Privacy Act Training Requirements Pursuant to the Federal Information Security Modernization Act of 2014



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

November 30, 2022

MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE FOR PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY

SUBJECT: Management Advisory: The DoD's Compliance with Privacy Act Training Requirements Pursuant to the Federal Information Security Modernization Act of 2014 (Report No. DODIG-2023-033)

The purpose of this management advisory is to provide DoD leadership with a DoD Office of Inspector General (DoD OIG) finding and recommendation specific to requirements in the Federal Information Security Modernization Act of 2014 (FISMA) relating to training on the Privacy Act of 1974, as amended (Privacy Act). We identified this finding during our FY 2021 review of the DoD's compliance with FISMA (Project No. D2021-D000CP-0034.000), which we announced on November 18, 2020. We conducted the work on this project with integrity, objectivity, and independence, as required by the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

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, a 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 the Department of Homeland Security.

As part of our FY 2021 independent review, we assessed selected portions of the DoD's Privacy Act training program and practices. We submitted the results of the overall effectiveness of the DoD's information security program and practices to the Office of Management and Budget and the Department of Homeland Security on October 28, 2021. We are issuing this advisory to report the results specific to DoD privacy training and to issue a recommendation for corrective action.

We provided a draft copy of this management advisory to DoD management and requested written comments on the recommendation. We considered management's comments on the draft when preparing the final advisory. These comments are included in the management advisory.

This management advisory contains one recommendation that we considered resolved. Therefore, as discussed in the Recommendation, Management Comments, and Our Response section, the recommendation remains open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, we will close the recommendation.

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

We appreciate the cooperation and assistance received during the review. If you have any questions, please contact me [redacted].

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

Background

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 law provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides 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 also establishes 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 information security policies and practices across the Government. FISMA requires that senior agency officials provide security for the information and information systems (information security program) 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. Federal agencies' information security programs are supported by security policy promulgated through the OMB, DHS, and risk-based standards and guidelines published by National Institute of Standards and Technology (NIST).

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

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 of their agency's information security program using annual IG FISMA reporting metrics.[1] The OMB, DHS, and Council of the Inspectors General on Integrity and Efficiency develop the IG FISMA reporting metrics, in consultation with the Federal Chief Information Officer Council.

FISMA Reporting Metrics

The FY 2021 OMB guidance included 66 IG FISMA reporting metrics.[2] The metrics were grouped into nine domains aligned under the five information security functions established by the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover.[3]

[1] OMB Memorandum M-21-02, "Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020.

[2] IG FISMA metrics are questions addressing various aspects of an organization's information security program.

[3] "FY 2021 IG FISMA Reporting Metrics," Version 1.1, May 12, 2021. The FY 2021 IG FISMA Reporting Metrics referenced public law, Federal requirements, and NIST guidance as the criteria for measuring an agency's information security program and practices.

The NIST Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise.[4] Table 1 describes the nine domains by function.

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

Table 1. Descriptions of NIST Cybersecurity Framework Functions and FISMA Domains

Function	Domain	Description
Identify	Risk Management	Risk management is the program and processes for 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.
Protect	Configuration Management	Configuration management consists of a collection of activities focused on 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 that management of those systems and data are 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.
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.
Respond	Incident Response	Incident response is a formal, focused, and coordinated approach to responding to cybersecurity incidents.
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.

Source: The DoD OIG.

[4] "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.

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 whether the policies and procedures are implemented and effective. Figure 1 shows the five-level IG FISMA maturity model.

Figure 1. IG FISMA Maturity Model

Source: FY 2021 IG FISMA Reporting Metrics.

IGs use a simple majority of the metric ratings to determine the maturity level for each domain, and then use the domain ratings 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 to adjust the rating along the scale accordingly. IGs could 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.

Scope and Methodology

We assessed the DoD's Privacy Act training program from November 2020 through September 2022. Specifically, we assessed whether the training met the requirements outlined in the FY 2021 IG FISMA Reporting Metrics for Metric 39, under the Protect function, within the Data Protection and Privacy domain. Metric 39 asks whether organizations ensure that privacy awareness training is provided to all individuals, and that the training includes role-based training.

To accomplish our review, we analyzed DoD Privacy Program policies and procedures relevant to the metric and the corresponding NIST Special Publication (SP) 800-53 control.[5] We reviewed key documents, such as instructions and regulations supporting DoD efforts relevant to the selected metric question on privacy training. We also interviewed personnel from the Privacy, Civil Liberties, and Freedom of Information Act Directorate, which is responsible for providing privacy guidance to DoD Components.

DoD Privacy Program

According to officials from the Privacy, Civil Liberties, and Freedom of Information Act Directorate, the DoD Privacy Program is decentralized. DoD Component heads are responsible for ensuring that their privacy program implements policies, procedures, and training in accordance with the Privacy Act and DoD guidance. Specifically, DoD Instruction 5400.11 requires DoD Components to establish and maintain comprehensive privacy and civil liberties programs that comply with applicable requirements and manage privacy risks, such as FISMA, NIST guidance, and the Privacy Act.[6] The Instruction provides the following key roles and responsibilities pertaining to the DoD Privacy Program.

DoD Chief Management Officer.[7] The DoD Chief Management Officer advises the Secretary of Defense and senior DoD leadership on the DoD Privacy and Civil Liberties programs, and is required to designate a Senior Agency Official for Privacy (SAOP) who has DoD-wide responsibility and accountability for developing, implementing, and maintaining a DoD-wide Privacy Program.

DoD Senior Agency Official for Privacy. The DoD SAOP oversees, coordinates, and facilitates the DoD's privacy and civil liberties compliance efforts and manages privacy risks associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) specific to DoD programs and information systems.[8] The DoD SAOP is the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

---

[5] 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 in Revision 4 to NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."

[6] DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019 (Incorporating Change 1, December 8, 2020).

[7] In the Deputy Secretary of Defense memorandum, "Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues," September 1, 2021, the Deputy Secretary disestablished the Office of the DoD Chief Management Officer effective October 1, 2021. As a result, the privacy responsibilities of the DoD Chief Management Officer were realigned to the newly established Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

[8] PII is information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual.

Privacy, Civil Liberties, and Freedom of Information Act Director.[9] The Director for Privacy, Civil Liberties, and Freedom of Information Act Directorate oversees and implements the DoD Privacy and Civil Liberties Programs and ensures that guidance, assistance, and subject matter expert support are provided to DoD Components in the implementation and execution of DoD Privacy and Civil Liberties Programs.

DoD Privacy Training Guidance

Although the DoD had privacy program policies and procedures in place for privacy training, the policies and procedures did not provide DoD Components a clear baseline for minimum content covered or frequency of required privacy training. Providing a baseline for privacy training helps to ensure personnel are aware of privacy program requirements, thereby enhancing the organization's ability to properly collect, maintain, use, and disseminate PII and protect it from unauthorized access.

Although the DoD had privacy program policies and procedures in place for privacy training, the policies and procedures did not provide DoD Components a clear baseline for minimum content covered or frequency of required privacy training.

Protect Function/Data Protection and Privacy Domain

For the Protect Function/Data Protection and Privacy Domain, we assessed 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?"

The DoD had privacy program policies and procedures in place that required its personnel to take privacy training. However, the DoD policies and procedures did not provide guidance specifying the minimum content or frequency for recurring basic privacy training and the minimum frequency for recurring role-based privacy training.[10] NIST SP 800-53, Revision 4 directs organizations to oversee basic privacy training and targeted, role-based privacy training at least annually and identifies potential content for privacy training, such as responsibilities under the Privacy Act, consequences of failing to carry out those responsibilities, data collection and use requirements, and privacy incident reporting.[11]

[9] According to Privacy officials, the Defense Privacy, Civil Liberties, and Transparency Division became the Privacy, Civil Liberties, and Freedom of Information Act Directorate when the Deputy Secretary of Defense disestablished the Office of the DoD Chief Management Officer.

[10] We did not review content of role-based privacy training because the DoD Components we reviewed did not track role-based training at the enterprise level where we conducted our review.

[11] Similar to Revision 4, NIST SP 800-53, Revision 5, directs organizations to provide literacy privacy training and role-based privacy training at an organizationally defined frequency and identifies potential content for literacy training such as understanding the need for privacy, user actions to maintain privacy, incident response, lessons learned from breaches, and handling of PII. Literacy is familiarity with, and the ability to apply, a core knowledge set of information.

DoD Instruction 5400.11 requires DoD Components to train personnel (military members, civilians, and contractors) on privacy rules of conduct, penalties for noncompliance, and incident response, mitigation, and reporting, and refers to DoD 5400.11-R for more detailed training guidance.[12] DoD 5400.11-R requires privacy training to include information on privacy laws, regulations, policies, and procedures governing DoD collection, maintenance, use, or dissemination of personal information. DoD 5400.11-R further states that DoD Components may establish orientation training providing a basic understanding of the DoD Privacy Program and are required to conduct privacy training as frequently as deemed necessary. However, DoD Instruction 5400.11 and DoD 5400.11-R do not specify the minimum content for recurring basic privacy training or the frequency needed for basic and role-based privacy training, as required by NIST guidance.

DoD Instruction 5400.11 also requires that DoD Components comply with OMB Memorandum M-17-12 and provide adequate training and awareness for employees and contractors on incident response, reporting, and mitigation.[13] OMB Memorandum M-17-12 requires that each agency develop training on identifying and responding to privacy breaches and that the training be provided to all personnel before accessing Federal information and information systems, and thereafter to be included in annual baseline privacy and security awareness training. However, DoD 5400.11-R does not require annual baseline privacy training for all personnel with access to DoD information or information systems. Instead, it only requires DoD Components to consider mandating annual privacy training. Although DoD Instruction 5400.11 and DoD 5400.11-R do not specify minimum content for basic privacy training, officials from the Privacy, Civil Liberties, and Freedom of Information Act Directorate explained that basic privacy training should include provisions of the Privacy Act, penalties for violating the act, information on the appropriate handling and safeguarding of PII, authorized uses of PII, and procedures to follow in the event of an incident or breach. The lack of a formal baseline for privacy training content hinders the DoD's ability to ensure that all DoD personnel receive adequate and consistent privacy awareness training. For example, without a baseline for training content, officials from the Privacy, Civil Liberties, and Freedom of Information Act Directorate are not able to determine the adequacy of basic privacy training used by DoD Components when responding to annual FISMA metrics.[14]

The lack of a formal baseline for privacy training content hinders the DoD's ability to ensure that all DoD personnel receive adequate and consistent privacy awareness training.

[12] DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

[13] OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017.

[14] The OMB collects annual SAOP metrics according to FISMA, the Privacy Act, and other laws, regulations, and policies. Each year, the OMB issues guidance instructing each SAOP to review the administration of their agency's privacy program and report compliance to the OMB.

Recommendation, Management Comments, and Our Response

Recommendation 1

We recommend that the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency revise DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019 (Incorporating Change 1, December 8, 2020), and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, to include the minimum content requirements and frequency for basic and role-based privacy training, as required by the National Institute of Standards and Technology guidance.

Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency Comments

The Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency agreed, stating that the DoD has a decentralized privacy program, and decisions about tailoring basic and role-based privacy training are made by the DoD Components based on Component-specific factors. The Assistant to the Secretary of Defense added that due to the creation of her position on September 1, 2021, her office is revising its issuances, including DoD Instruction 5400.11, to reflect the new organizational structure and roles of the DoD privacy program. She noted that her office provides privacy training courses that cover key topics, such as the Privacy Act, safeguarding PII, PII breaches, the protection of social security numbers, and the Fair Information Practice Principles, which Privacy Officers can use in their Component-level privacy training programs. She also explained that the updates to DoD Instruction 5400.11 would address our recommendation by providing guidance to address how Senior Component Officials for Privacy best determine the frequency and content of their Component's basic and role-based training. She said that the updates should be completed by the fourth quarter of FY 2023.

Our Response

Comments from the Assistant to the Secretary of Defense addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Assistant to the Secretary of Defense provides the revised DoD Instruction 5400.11 and we verify that it includes the minimum content requirements and frequency for basic and role-based privacy training as required by NIST guidance.

Management Comments

Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency

ASSISTANT TO THE SECRETARY OF DEFENSE FOR
PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

November 2, 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL

SUBJECT: DoD Office of Inspector General (DoDIG) Management Advisory: The DoD's Compliance with Privacy Act Training Requirements Pursuant to the Federal Information Security Modernization Act of 2014

Thank you for the Management Advisory examining DoD's privacy training and the accompanying recommendation. I concur with your recommendation to revise DoD Instruction (DoDI) 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019 (Incorporating Change 1, December 8, 2020), and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, to more clearly address how DoD Components should determine the content requirements and frequency for basic and role-based privacy training.

DoD policy requires all DoD Components to establish and maintain a comprehensive privacy and civil liberties programs to comply with applicable requirements and requires that DoD Components designate a Senior Component Officials for Privacy (SCOP) to implement and oversee the Component privacy programs. Because DoD operates such a decentralized privacy program, decisions about how best to tailor basic and role-based privacy training are to be made by the DoD Components. The intent is that each SCOP makes these determinations for their organization. When making these decisions, SCOPs are informed by factors such as: the Component's unique legal authorities, the nature and extent of personally identifiable information (PII) and Privacy Act records maintained, the organizational and workforce structure, organizational training strategy, and any mission-specific privacy laws that may apply, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to the creation of my position as the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency on September 1, 2021, my Office is revising its issuances, including DoDI 5400.11, to reflect the new organizational structure and roles of the DoD privacy program. At that time, I intend to modify DoDI 5400.11 to provide more specific guidance for SCOPs, such as the factors above, on how best to determine the frequency and content of their Component's basic and role-based training to satisfy the DoDIG recommendation. I expect the update to DoDI 5400.11 to be completed during Fiscal Year 2023.

I am proud of the privacy training occurring at all levels of the DoD, and always welcome recommendations to improve the privacy awareness of our workforce and the strength of our privacy program. My Office offers both live and recorded privacy training courses and completion certificates covering key topics in depth, including the Privacy Act, safeguarding PII, PII breaches, the protection of Social Security Numbers, and the Fair Information Practice Principles. Component privacy offices may adapt the training materials to use locally in their Component-level privacy training programs. Some Components mandated their workforce take

Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (cont'd)

some of our courses to satisfy the Component's basic privacy training requirement. DoD CIO's mandatory annual cyber awareness training also addresses privacy by focusing on evolving cyber threats and requirements issued by Congress and the Office of Management and Budget. The training also reinforces best practices to protect privacy. All DoD information system users are required to complete cyber awareness instruction as a condition of initial system access, and thereafter annual refresher training as required by the Office of Personnel Management.

Thank you again for the opportunity to respond to this Management Advisory. Please refer any questions about this matter to [redacted]

CHUNG.JOO.Y [redacted]

Joo Y. Chung

2


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at 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; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098