

JUNE 7-8, 2011

TMA Privacy Weekly

TMA Privacy and Civil Liberties Office
2011 DATA PROTECTION SEMINAR



Privacy Impact Assessments



Privacy Impact Assessments

Purpose

The purpose of this presentation is to provide a high-level overview of Privacy Impact Assessments (PIAs), the TRICARE Management Activity (TMA) PIA process, the DoD PIA template (DD Form 2930), and responsibilities regarding completion of the PIA.



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Objectives

- Upon completion of this presentation, you should be able to:
 - Explain PIAs and how they help safeguard personally identifiable information (PII) and protected health information (PHI)
 - Define basic PIA terms
 - Explain the DoD PIA policy
 - Explain the DoD PIA template
 - Explain the PIA process
 - Discuss PIA after-action items



Privacy Impact Assessments

What is a PIA?

- A PIA is an analysis of how PII is safeguarded in an information technology (IT) system
- A PIA can be performed at any time during a system's life cycle
 - PIAs can be performed on a “conceptual system”
 - PIAs should be started in the earliest stages of the system life cycle
 - PIAs are performed on legacy systems



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

What is a PIA? (continued)

- PIAs are conducted to:
 - Ensure that systems conform to privacy requirements
 - Assess risks
 - Mitigate potential risks
- Four main goals of a PIA are:
 - Verification and validation
 - Accountability
 - Consistency
 - Remediation



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

What is a PIA? (continued)

- A PIA must be a standalone document
- A PIA must be consistent with a system's security documentation
- A PIA must be consistent with applicable System of Records Notices (SORNs)
- A PIA is one way that federal agencies inform the public on uses of their PII



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Why PIAs Are Required – Federal and DoD

- E-Government Act of 2002 § 208, December 17, 2002
- Federal Information Security Management Act (FISMA)
- Office of Management and Budget (OMB)
 - OMB Memorandum M-03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
 - OMB Circular A-11: Capital Planning Process/Exhibit 300s
- DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance”, February 12, 2009



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

PIA Requirements

- Federal agency PIA requirements
 - Section 208 of the E-Government Act of 2002 requires all agencies to conduct PIAs for all new or substantially changed information systems that collect, maintain, or disseminate PII on the public
- DoD PIA requirements
 - DoD Instruction 5400.16 expands the coverage to include federal personnel, contractors, and foreign nationals employed at United States military facilities internationally



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Why Are PIAs Required?

- DoD takes its responsibility to safeguard PII/PHI and to prevent its theft, loss, or compromise seriously
- DoD is addressing privacy and security challenges through many initiatives, including PIAs
 - Ensuring that DoD employees and contractors are aware of their privacy responsibilities
- Completion of the PIA is a part of the DoD Information Assurance Certification and Accreditation Process (DIACAP)
 - Failure to complete a PIA may result in delays to a system's certification



HEALTH AFFAIRS



TRICARE®

TRICARE
Management Activity

PIA Terminology

- Personally identifiable information (PII)
 - Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which 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, etc., including any other personal information which is linked or linkable to an individual



PIA Terminology (continued)

- DoD information system
 - Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes Automated Information System applications, enclaves, outsourced IT-based processes, and platform IT interconnections
- Electronic collection
 - Any collection of information enabled by IT



PIA Terminology (continued)

- Federal personnel
 - Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits)



Privacy Impact Assessments

Who is Responsible for Completing a PIA?

- System Program Manager has ultimate responsibility for the PIA
- Collaborative effort
 - System manager
 - System developer
 - System support team
 - Functional expert
 - Government representative
- TMA Privacy and Civil Liberties Office (Privacy Office) PIA Analyst will be available to assist with questions



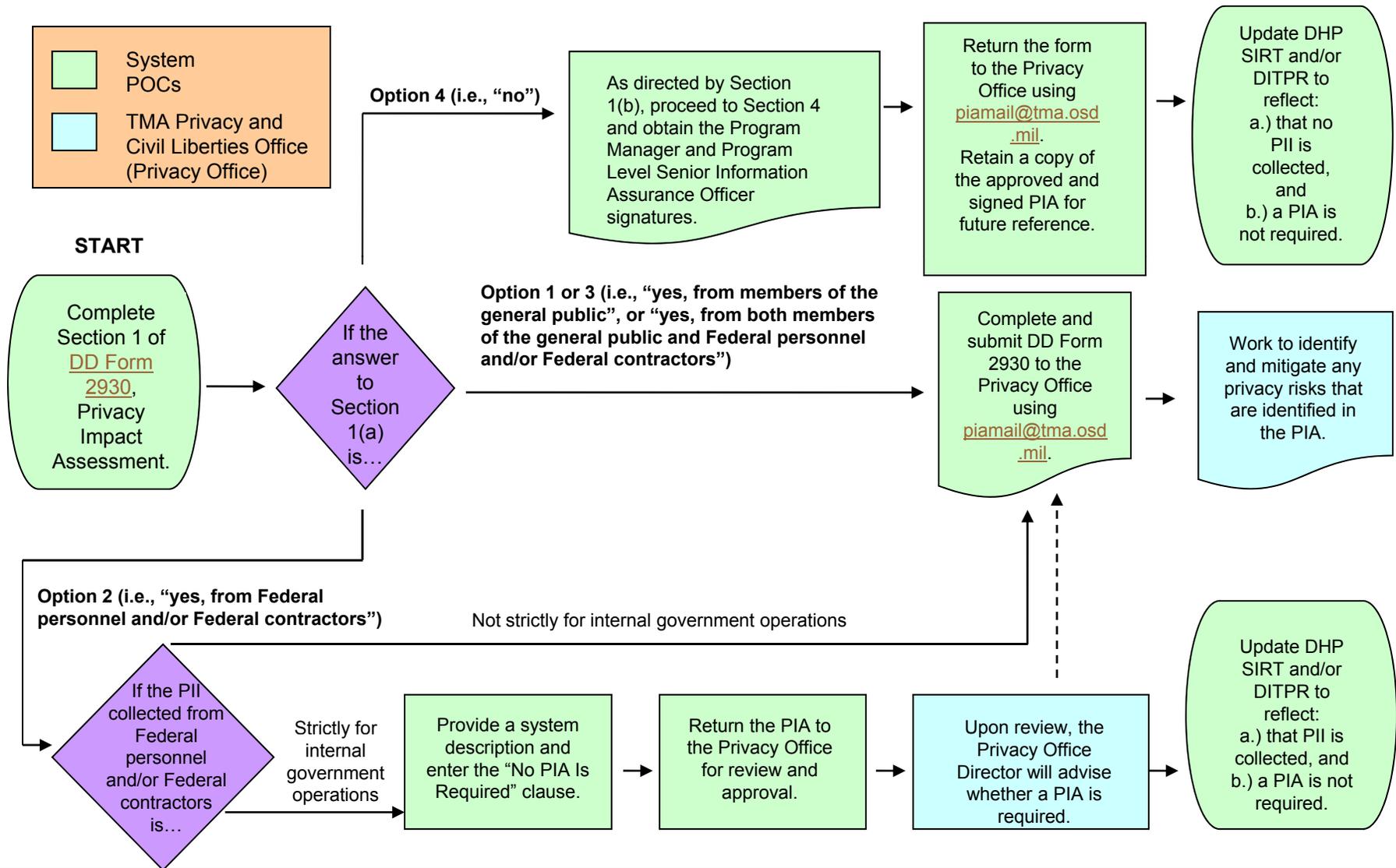
HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Overview of the PIA Process



Privacy Impact Assessments

Overview of the PIA Process (continued)

- Key information includes:
 - System description: purpose, boundaries, etc.
 - System development life cycle certification and accreditation (C&A) status
 - PII maintained in the system
 - Categories of individuals



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Overview of the PIA Process (continued)

- Key points include:
 - Privacy Act of 1974 compliance
 - Collecting PII from sources other than directly from individuals (databases, Web sites, etc.)
 - Populating PII for other resources (databases, Web sites, etc.)
 - Sharing or disclosing PII outside the service
 - Computer Matching and Privacy Protection Act agreements
 - Individual choice and notification



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Overview of the PIA Process (continued)

- Key resources include:
 - Security control assessments
 - Contingency plans
 - System and data backup plans
 - Password controls
 - Incident response plans
 - Physical controls
 - Controls on the use of mobile computing devices, removable storage media, remote access



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Overview of the PIA Process (continued)

- Signatures may include:
 - Preparing official – a government employee
 - Component Senior Information Assurance Officer
 - Component Privacy Officer
 - Component Chief Information Officer



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments

Overview of the PIA Process (continued)

- After-action items
 - File copy kept in Privacy Office
 - PIAs (section 1 and 2) are posted to the Privacy Office Web site
- Create a plan of action to mitigate identified risks
- Keep Privacy Office informed – PIAmail@tma.osd.mil
- PIA review and update
 - In conjunction with C&A
 - Three years from date of approval
 - Significant system change or a change in privacy or security posture



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessments Summary

- You should now be able to:
 - Explain PIAs and how they help safeguard PII and PHI
 - Define basic PIA terms
 - Explain the DoD PIA policy
 - Explain the DoD PIA template
 - Explain the PIA process
 - Discuss PIA after-action items



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessment Resources

- E-Government Act of 2002 § 208, December 17, 2002
- Office of Management and Budget Memorandum 03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance”, February 12, 2009
- DD Form 2930, DoD PIA template
- E-mail PIAmail@tma.osd.mil for subject matter questions
- <http://www.tricare.mil/tma/privacy/pias.aspx>



HEALTH AFFAIRS



TRICARE
Management Activity

Privacy Impact Assessment

Resources (continued)

- DoD 5400.11-R, “DoD Privacy Program”, May 14, 2007
- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- To subscribe to the Privacy Office E-News, go to:
<http://www.tricare.mil/tma/privacy/maillinglist.aspx>



HEALTH AFFAIRS



TRICARE
Management Activity