Report No. D-2010-058 May 14, 2010

Inspector General
United States
Department of Defense


# Selected Controls for Information Assurance at the Defense Threat Reduction Agency

## Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

## Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704


## Acronyms and Abbreviations

| | |
|---|---|
| ASD(NII)/DOD CIO | Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer |
| CND-SP | Computer Network Defense-Service Provider |
| DAA | Designated Approving Authority |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DTRA | Defense Threat Reduction Agency |
| FISMA | Federal Information Security Management Act |
| GAO | Government Accountability Office |
| IA | Information Assurance |
| IAM | Information Assurance Management |
| IASAE | Information Assurance System Architect and Engineer |
| IAT | Information Assurance Technical |
| NIST | National Institute on Standards and Technology |

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

MAY 14 2010

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND INFORMATION INTEGRATION)/DOD CHIEF INFORMATION OFFICER
ASSISTANT TO THE SECRETARY OF DEFENSE FOR NUCLEAR AND CHEMICAL AND BIOLOGICAL DEFENSE PROGRAMS
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY

SUBJECT: Selected Controls for Information Assurance at the Defense Threat Reduction Agency (Report No. D-2010-058)

We are providing this report for your information and use. We considered management comments on a draft of this report when preparing the final report. The Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer and the Director, Defense Threat Reduction Agency, comments conformed to the requirements of DOD Directive 7650.3; therefore, we do not require additional comments.

We appreciate the courtesies extended to the staff. Please direct questions to Mr. Robert F. Prinzbach II at (703) 604-8907 (DSN 664-8907).

Alice F. Carey
Acting Assistant Inspector General
Readiness, Operations, and Support

# Results in Brief: Selected Controls for Information Assurance at the Defense Threat Reduction Agency

## What We Did

The objectives of this audit were to determine whether personnel responsible for information assurance were certified in accordance with regulations and whether information system accounts were disabled when employees left the agency. We reviewed designations of information assurance personnel and their corresponding certification status. We also reviewed whether information system accounts were disabled in a timely manner.

## What We Found

As of August 2009, the date of the Defense Threat Reduction Agency (DTRA) response to DOD for the 2009 Federal Information Security Management Act report, DTRA needed 80 additional information assurance personnel to be certified to meet December 2009 certification milestones. DTRA also did not follow regulations for identification and certification of information assurance personnel. These conditions occurred because DTRA did not have adequate internal controls in place and did not adequately oversee its information assurance workforce. As a result, the DTRA information assurance workforce may not have an adequate understanding of the concepts, principles, and applications of information assurance to enhance the protection and availability of information systems and networks. In addition, data made available by DTRA to DOD and Congress were inaccurate and incomplete. DTRA did not disable 17 accounts within 9 information systems and networks after personnel left the agency. Additionally, of 87 disabled accounts that we reviewed, 84 accounts remained active 5 days after the personnel left the agency, and 66 accounts remained active after 30 days. This occurred because internal controls were not in place to notify information system representatives when personnel left the agency and to ensure that system administrators review inactive accounts in accordance with DTRA guidance. As a result, unauthorized individuals could have accessed sensitive information within agency information systems and networks.

## What We Recommend

We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer (ASD[NII]/DOD CIO) modify DOD 8570.01-M to require all DOD information assurance personnel to authorize release of their certification qualifications in the Defense Workforce Certification Application. We also recommend that the Director, DTRA:

- develop and implement an adequate process to identify information assurance personnel and monitor their certification status,
- notify system representatives when personnel leave the agency, and
- review active accounts at least monthly and suspend inactive accounts in accordance with DTRA guidance.

## Management Comments and Our Response

The Acting Deputy Assistant Secretary of Defense (Identity and Information Assurance) in the Office of the ASD(NII)/DOD CIO and the Director, DTRA, agreed with the recommendations. Management comments were responsive to the recommendations. No additional comments are required.

## Recommendations Table

| Management | Recommendations Requiring Comment | No Additional Comments Required |
|---|---|---|
| Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer | | A.3 |
| Director, Defense Threat Reduction Agency | | A.1.a-g, A.2, B.1, and B.2 |

# Table of Contents

# Introduction

## Objectives

The objectives of this audit were to determine whether Defense Threat Reduction Agency (DTRA) personnel responsible for information assurance (IA) were certified in accordance with regulations and whether information system accounts were disabled when employees left the agency. We reviewed designations of information assurance personnel and their corresponding certification status. We also reviewed whether information system accounts were disabled in a timely manner. See the Appendix for a discussion of the scope and methodology and prior coverage related to the objectives.

## Background

DTRA is responsible for safeguarding the United States and its allies from weapons of mass destruction by providing capabilities to reduce, eliminate, and counter the threat and mitigate their effects. DTRA is a DOD Agency that reports to the Under Secretary of Defense for Acquisition, Technology, and Logistics through the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs.

The Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD[NII]/DOD CIO) is the principal staff assistant and advisor to the Secretary of Defense for DOD information and information technology matters including IA.

The Federal Information Security Management Act (FISMA) of 2002 was passed as part of the E-Government Act of 2002 (Public Law 107-347). FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Each Federal agency (for example, DOD) is required to report annually to Congress on compliance with requirements and the adequacy and effectiveness of information security policies, procedures, and practices.

DOD Directive 8500.01E, "Information Assurance," October 24, 2002, establishes policy to achieve IA across DOD. DOD Instruction 8500.02, "Information Assurance Implementation," February 6, 2003, implements policy and prescribes procedures for applying integrated, layered protection of DOD information systems and networks. DOD Instruction 8500.02 defines IA as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

## Review of Internal Controls

DOD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006, requires DOD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control

weaknesses for DTRA. DTRA did not have the following internal controls to adequately identify their IA workforce and monitor the IA workforce certification status: an ongoing process to identify personnel that had IA responsibilities and monitor whether the personnel obtained the appropriate certifications, a central repository of IA certifications, and an adequate tracking tool to identify IA personnel and track their progress in obtaining the appropriate certifications. DTRA did not have internal controls to ensure that system representatives for all DTRA systems were notified when personnel left the agency to enable the system representatives to promptly disable system accounts. Additionally, DTRA did not have internal controls in place to ensure that inactive accounts were disabled in accordance with agency guidance. Implementing recommendations A.1 and A.2 will improve DTRA processes to identify its IA workforce and monitor the IA workforce certification status. Implementing recommendations B.1 and B.2 will improve DTRA processes to disable accounts for personnel that leave the agency. These improvements will reduce potential vulnerabilities within DTRA's information systems. We will provide a copy of the report to the senior official responsible for internal controls in DTRA and in the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

# Finding A. Identification and Certification of Information Assurance Personnel

As of August 2009, the date of the DTRA response to DOD for the 2009 FISMA report, only 35.2 percent of DTRA IA personnel met certification requirements, and DTRA needed 80 additional IA personnel to be certified to meet December 2009 certification milestones. Additionally, DTRA personnel did not follow regulations for identification and certification of personnel having IA responsibilities. DTRA:

- reported inaccurate information for IA personnel onboard and certified in its response to the DOD data call for the 2009 FISMA report,
- did not properly input data on IA personnel in the Defense Civilian Personnel Data System, and
- did not require that its IA workforce authorized release of their certification information in the Defense Workforce Certification Application.

These conditions occurred because DTRA did not provide adequate oversight of its IA workforce. DTRA:

- did not have an adequate process in place to identify IA personnel and monitor whether IA personnel obtained the appropriate certifications and
- did not ensure that contract language requiring all contractor personnel to be certified was added to contracts for IA services.

As a result, DTRA's IA workforce may not have an adequate understanding of the concepts, principles, and applications of IA to enhance the protection and availability of DTRA's information systems and networks. Further, DOD and Congress did not have accurate information on DTRA's IA workforce and progress towards meeting certification requirements established by DOD guidance.

## IA Workforce Background

An IA workforce consists of personnel that focus on the operation and management of IA capabilities for DOD systems and networks. The workforce ensures that adequate security measures and established IA policies and procedures are applied to all information systems and networks.

DOD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, establishes policy and assigns responsibility for DOD IA training, certification, and workforce management. DOD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, implements DOD Directive 8570.01 and provides guidance for the identification and categorization of positions and certification of personnel conducting IA functions, and establishes IA workforce oversight and management reporting requirements. The Defense-Wide Information Assurance Program of the ASD(NII)/DOD CIO provides IA

workforce management oversight and coordination for the requirements established in DOD 8570.01-M. DOD 8570.01-M applies to all civilian, military, and contractor personnel that perform IA functions.

DOD 8570.01-M requires all DOD Components to identify their IA positions and the personnel that fill those positions. The DOD Components must designate each IA position with an IA category or specialty. IA categories and specialties are further divided into levels based on functional skill requirements and/or system environment focus. IA categories include:

- IA technical (IAT) Levels I, II, and III and
- IA management (IAM) Levels I, II, and III, as well as the Designated Approving Authority (DAA).

IA specialties include:

- IA Systems Architect and Engineer (IASAE) Levels I, II, and III and
- Computer Network Defense Service Provider (CND-SP):
    - analyst,
    - infrastructure support,
    - incident responder,
    - auditor, and
    - manager.

Personnel that fill an IA position (except a DAA position) are required to obtain a specific baseline certification as established by DOD 8570.01-M. According to DOD 8570.01-M, baseline certifications are approved certifications that DOD uses to establish technical and management IA skills across DOD. Further, DOD 8570.01-M requires that personnel designated in some categories and specialties also obtain a computing environment certification. Computing environment certifications ensure that personnel can effectively apply IA requirements to hardware and software systems. Personnel that fill DAA positions are required to complete an approved DAA-related certification course. See Table 1 for the certifications required for IA categories and specialties.

**Table 1. Certifications Required for IA Categories and Specialties**

| Category/Specialty | Baseline Certification Required | Computing Environment Certification Required |
|---|---|---|
| IAT Levels I, II, and III | Yes | Yes |
| IAM Levels I, II, and III | Yes | No |
| IASAE Levels I, II, and III | Yes | No |
| CND-SP analyst | Yes | Yes |
| CND-SP infrastructure support | Yes | Yes |
| CND-SP incident responder | Yes | Yes |
| CND-SP auditor | Yes | Yes |
| CND-SP manager | Yes | No |

DOD 8570.01-M establishes milestones that DOD Components must meet. Specifically, DOD Components are required to:

- identify their IA workforce positions and fill 10 percent of the IA positions with certified personnel by December 31, 2007;
- fill a total of 40 percent of their IA positions with certified personnel by December 31, 2008;
- fill a total of 70 percent of their IA positions with certified personnel by December 31, 2009;
- fill all IAT and IAM category positions with certified personnel by December 31, 2010; and
- fill all CND-SP and IASAE specialty positions with certified personnel by December 31, 2011.

## DOD Required Certification Milestones and Reporting of Information Assurance Personnel

As of August 2009, only 35.2 percent of DTRA IA personnel met certification requirements, and DTRA needed 80 additional IA personnel to be certified to meet December 2009 certification milestones. Additionally, DTRA personnel did not follow established guidance for identification and certification requirements of personnel having IA responsibilities. DTRA:

- reported inaccurate information for IA personnel onboard and certified in its response to the DOD data call for the 2009 FISMA report,
- did not properly input data on IA personnel in the Defense Civilian Personnel Data System, and
- did not require that its IA workforce authorized release of their certification information in the Defense Workforce Certification Application.

### *DTRA Compliance with DOD Certification Milestones*

As of August 2009, only 35.2 percent of DTRA IA personnel met certification requirements, and DTRA needed 80 additional IA personnel to be certified to meet December 2009 certification milestones. DOD 8570.01-M required DOD Components to fill a total of 40 percent of the IA positions with certified personnel by the end of 2008 and fill a total of 70 percent of the positions with certified personnel by the end of 2009. In the 2008 IA Workforce Improvement Program Report sent to ASD(NII)/DOD CIO, DTRA reported that 45 percent of its personnel with IA responsibilities obtained certifications. Based on DTRA's reported numbers, DTRA exceeded the required milestone for 2008. However, between the end of 2008 and August 2009, DTRA's number of certified personnel decreased. In August 2009, DTRA reported in its official response for the 2009 FISMA report, that only 31.2 percent of its IA workforce was certified. DTRA attributed the decrease to a change in a contractor for information technology services at DTRA. However, as we discuss later in the report, all of the personnel included in the contract should have been certified prior to beginning work at DTRA. As of August 2009, we verified that 35.2 percent of the DTRA IA workforce had

the appropriate baseline certifications. DTRA needed 80 additional personnel to be certified prior to the end of 2009 to meet the 70 percent milestone as required by DOD 8570.01-M.

We did not determine whether personnel designated in the IAT category or CND-SP specialty obtained the appropriate computing environment certifications because the DOD Components did not have to include the number of personnel that held a computing environment certification in the 2009 FISMA response. However, according to FISMA instructions, the 2009 IA Workforce Improvement Program Report, due on December 31, 2009, requires that DOD Components report the number of personnel that have obtained computing environment certifications. Based on documentation that we received, a substantially lower number of DTRA personnel have obtained both the IA baseline and computing environment certifications. Once FISMA requires agencies to report this information, DTRA's percentage of personnel that are adequately certified may decrease significantly.

## *DTRA's Response to DOD Data Call for 2009 FISMA Report*

DTRA reported inaccurate information for IA personnel onboard and certified in its response to the DOD data call for the 2009 FISMA report. DTRA reported in August 2009 that it had 205 IA personnel, of which 64 were certified (31.2 percent). However, we found that DTRA had 230 IA personnel, of which 81 were certified (35.2 percent). DTRA's August 2009 report had multiple errors and was incomplete. Table 2 provides a summary of DTRA's FISMA response and our results of verified IA personnel and certifications.

**Table 2. DTRA IA Personnel and Personnel Certified**

| | **DTRA 2009 FISMA Response** | | | **Inspector General-Verified Data** | | |
|---|---|---|---|---|---|---|
| **Category** | **# IA Personnel** | **# Certified** | **% Certified** | **# IA Personnel** | **# Certified** | **% Certified** |
| IAT I | 28 | 5 | 17.9% | 32 | 7 | 21.9% |
| IAT II | 156 | 52 | 33.3% | 158 | 63 | 39.9% |
| IAT III | 4 | 3 | 75.0% | 4 | 3 | 75.0% |
| IAM I | 1 | 0 | 0.0% | 1 | 0 | 0.0% |
| IAM II | 11 | 2 | 18.2% | 12 | 1 | 8.3% |
| IAM III | 4 | 1 | 25.0% | 7 | 2 | 28.6% |
| CND-SP | 0 | 0 | 0.0% | 13 | 4 | 30.8% |
| IASAE | 0 | 0 | 0.0% | 2 | 0 | 0.0% |
| DAA | 1 | 1 | 100.0% | 1 | 1 | 100.0% |
| **Total** | **205** | **64** | **31.2%** | **230** | **81** | **35.2%** |

We identified that the IA workforce information for DTRA within the 2009 FISMA response was inaccurate and incomplete.

We identified the following types of errors:

- mathematical inaccuracies,
- IA personnel and certifications excluded from 2009 FISMA response,
- incorrect category or specialty for personnel and certifications, and
- improper certifications for IA category.

## Mathematical Accuracy

DTRA personnel miscounted the number of IA personnel in the DTRA IA workforce, as well as the number of IA personnel that were certified. We initially attempted to reconcile the 2009 FISMA response data to documentation that DTRA provided; however, the documentation did not always match DTRA's 2009 FISMA response.

We found 12 mathematical errors in DTRA's reported numbers for IA personnel. As a result, DTRA had undercounted the number of IA personnel by four. Additionally, we found one mathematical error in DTRA's reported numbers for certified personnel resulting in an understatement of one certified person.

## Additional IA Personnel and Certifications

DTRA should have included an additional 21 IA personnel as part of the 2009 FISMA response. Specifically, we identified 19 additional IA personnel and 19 additional certifications that DTRA had not identified prior to their FISMA response. DTRA counted certifications for two contractor personnel that were not included in the number of personnel within the IA workforce. DTRA personnel agreed that those two personnel should have been included in the number of personnel within the IA workforce in the FISMA response.

## Categorization of Personnel and Certifications

DTRA did not appropriately categorize personnel and corresponding certifications in their 2009 FISMA response. We learned from personnel with oversight responsibilities of the Network Operations Support Center that 12 DTRA personnel designated at the IAT II Level in the FISMA response were actually performing CND-SP functions. Additionally, 4 of the 12 personnel had certifications, which DTRA also counted at the IAT II Level on the 2009 FISMA response. DOD 8570.01-M was modified on May 15, 2008, to require DOD Components to identify any personnel performing CND-SP or IASAE functions in its FISMA response.

## Appropriateness of Certifications for IA Category and Level

Three personnel identified on the 2009 FISMA response did not have the correct certification for their designated category and level, which caused the number of certified personnel to be overstated by three. For example, one of the employees at the IAT II Level had obtained the Certified Information Security Management certification. A DTRA official stated that they included this certification in the FISMA response; however, the DOD 8570.01-M requires personnel at the IAT II Level to obtain a Global Information Assurance Certification Security Essentials Certification, Security+

certification, Security Certified Network Professional certification, or System Security Certified Practitioner certification.

Table 3 identifies the discrepancies in IA personnel data included in the 2009 FISMA response.

**Table 3. IA Personnel Data Discrepancies in 2009 FISMA Response**

| Category | DTRA FISMA Response | Math Errors | IA Personnel Excluded | Incorrect Category/ Specialty | Verified |
|---|---|---|---|---|---|
| IAT I | 28 | 4 | 0 | 0 | **32** |
| IAT II | 156 | -2* | 16 | -12 | **158** |
| IAT III | 4 | 0 | 0 | 0 | **4** |
| IAM I | 1 | 0 | 0 | 0 | **1** |
| IAM II | 11 | 1 | 0 | 0 | **12** |
| IAM III | 4 | 1 | 2 | 0 | **7** |
| CND-SP | 0 | 0 | 1 | 12 | **13** |
| IASAE | 0 | 0 | 2 | 0 | **2** |
| DAA | 1 | 0 | 0 | 0 | **1** |
| **Total** | **205** | **4** | **21** | **0** | **230** |

* Result of a DTRA overcount of the number of contractors by four and an undercount of the number of civilians by two.

Table 4 identifies the discrepancies in IA certifications included in the 2009 FISMA response.

**Table 4. IA Certifications Discrepancies in 2009 FISMA Response**

| Category | DTRA FISMA Response | Math Errors | Certifications Excluded | Incorrect Category/ Specialty | Improper Certificate for Category | Verified |
|---|---|---|---|---|---|---|
| IAT I | 5 | 1 | 1 | 0 | 0 | **7** |
| IAT II | 52 | 0 | 17 | -4 | -2 | **63** |
| IAT III | 3 | 0 | 0 | 0 | 0 | **3** |
| IAM I | 0 | 0 | 0 | 0 | 0 | **0** |
| IAM II | 2 | 0 | 0 | 0 | -1 | **1** |
| IAM III | 1 | 0 | 1 | 0 | 0 | **2** |
| CND-SP | 0 | 0 | 0 | 4 | 0 | **4** |
| IASAE | 0 | 0 | 0 | 0 | 0 | **0** |
| DAA | 1 | 0 | 0 | 0 | 0 | **1** |
| **Total** | **64** | **1** | **19** | **0** | **-3** | **81** |

## *IA Personnel Data in the Defense Civilian Personnel Data System*

DTRA did not properly input data on IA personnel in the Defense Civilian Personnel Data System. DOD 8570.01-M requires DOD Components to enter information into the Defense Civilian Personnel Data System for civilian personnel with IA responsibilities. Further, the Director, Civilian Personnel Management Service, and the Under Secretary of Defense for Personnel and Readiness instructed DOD Components in June 2007 and August 2008, respectively, to enter data into the Defense Civilian Personnel Data System for those civilian personnel with IA responsibilities. As of July 2009, personnel from the Civilian Personnel Management Service stated that they were unable to identify any IA data for DTRA civilians within the Defense Civilian Personnel Data System and that DTRA should designate these positions. We met with DTRA personnel who are responsible for submitting information to the Defense Logistics Agency so the information could be put in the system. The personnel stated that they had not received the required information from the DTRA personnel responsible for the IA workforce program. Therefore, as of September 2, 2009, DTRA had not provided IA information to the Defense Logistics Agency so the information could be put in the system. The Under Secretary of Defense for Personnel and Readiness emphasized in his August 2008 memorandum the importance of entering proper and accurate data into the Defense Civilian Personnel Data System by stating that it is "paramount to accurate workforce management, analysis, and reporting." Additionally, the 2009 FISMA guidance states that the Defense Civilian Personnel Data System will be used for reporting the status of all Component civilian positions and personnel for the 2009 IA Workforce Improvement Program annual report due on December 31, 2009. DTRA should populate the required fields for those civilians with IA responsibilities to comply with DOD requirements and to better track IA personnel.

## *Information in the Defense Workforce Certification Application*

DTRA did not ensure that its IA workforce authorized release of certification information in the Defense Workforce Certification Application. A document published by the Defense Information Systems Agency stated that IA workforce personnel must access the Defense Workforce Certification Application and authorize the release of their certification information from the certification vendor to DOD. The Defense Information Systems Agency document stated that releasing the certification status to DOD using the Defense Workforce Certification Application is the official means of notifying DOD of their certification status, and that the application is the official source of IA certification information for civilian, military, and contractor personnel. The application is intended to populate personnel databases, such as the Defense Civilian Personnel Data System with information. This would serve as verification that personnel, particularly civilians, have in fact obtained their certifications. However, DOD 8570.01-M makes no mention of the application. Instead, DOD 8570.01-M states that "all personnel must agree to release their certification qualification(s) to the Department of Defense." If the ASD(NII)/DOD CIO wants to mandate that DOD Components use the Defense Workforce Certification Application, it should establish policy or modify DOD 8570.01-M. Additionally, DTRA should require their IA workforce to authorize release of their certification information using the Defense Workforce Certification Application.

# DTRA Oversight of IA Workforce

DTRA did not meet the certification milestones established by DOD 8570.01-M and did not accurately report its IA personnel and certification progress in the 2009 FISMA response or to DOD because DTRA did not adequately oversee its IA workforce. Specifically, DTRA:

- did not have an adequate process in place to identify IA personnel and monitor whether the IA personnel obtained the appropriate certifications and
- did not ensure that contract language requiring all contractor personnel to be certified was added to contracts for IA services.

## *Process Used to Identify IA Personnel and Monitor Certifications*

DTRA did not have an adequate process in place to identify IA personnel and monitor whether the IA personnel obtained the appropriate certifications. Specifically, DTRA did not:

- have an ongoing process in place to identify personnel that had information assurance responsibilities and monitor whether the personnel obtained the appropriate certifications,
- track whether new personnel obtained the required certifications,
- maintain a central repository of IA certifications, and
- have an adequate tool to identify IA personnel and track their progress in obtaining the appropriate certifications.

### Ongoing Process to Identify IA Workforce and Monitor Certifications

DTRA did not have an ongoing process in place to identify personnel that had IA responsibilities and monitor whether those personnel obtained the appropriate certifications. The DTRA official responsible for compiling IA personnel data stated that DTRA performed a data call in early July 2009 asking each program manager to identify personnel within their area that had IA responsibilities. The DTRA official stated that she did not receive many responses. Further, of the information that DTRA personnel did have, DTRA had not verified the information until 2 weeks before the 2009 FISMA response was due. We believe this contributed to some of the errors we found in the FISMA response. DTRA could become cognizant of their IA workforce by establishing an ongoing process to obtain feedback from designated points of contact throughout the agency to identify when new IA personnel come onboard and to know which of the current personnel perform IA functions. In addition, this process would provide more timely notice of personnel who had recently obtained the appropriate IA certifications. Further, DTRA personnel responsible for identifying the IA workforce should verify the information provided by these points of contact.

### Tracking of New Personnel

DTRA did not track whether new civilian and military personnel obtained the required certifications within 6 months. DOD 8570.01-M requires that IA civilian and military personnel obtain the appropriate certifications within 6 months of beginning their positions unless a waiver is granted. If personnel do not obtain the appropriate

certifications within the timeframe, they are not permitted to execute the responsibilities of the position or not permitted privileged system access. According to the Defense-Wide Information Assurance Program, personnel must be certified within 6 months of beginning a job, even when switching from one internal position to another. The DTRA official responsible for compiling IA personnel data stated that DTRA does not track arrival dates for personnel with IA responsibilities. DTRA should identify and track whether new civilian and military information assurance personnel obtain the appropriate certifications within 6 months of beginning work in an information assurance position in accordance with DOD 8570.01-M.

DTRA and contractor personnel also did not ensure that one contractor provided certified IA contractor personnel prior to beginning work at DTRA. One of the seven contracts that provided for personnel with IA responsibilities included a required Defense Federal Acquisition Regulation Supplement (DFARS) clause in the contract language, which requires IA contractor personnel to be certified in accordance with DoD 8570.01-M. However, based on information provided by a contractor representative, neither the contractor nor the contracting officer ensured that the IA contractor personnel were certified prior to beginning work at DTRA.

DFARS 252.239-7001, "Information Assurance Contractor Training and Certification," includes the clause that requires the contractor to provide a certified IA workforce. DOD 8570.01-M requires contractor personnel performing IA functions to be "appropriately certified prior to being engaged" and states that the contracting officer should ensure that contractor personnel are appropriately certified.

According to a file obtained from the contractor used to monitor the certification status of its contractor personnel, 57 personnel of 124 (or 46 percent) had the appropriate certifications as of August 2009. According to the contractor, as of September 2009, the contractor increased the number of its own contractor personnel with IA baseline certifications to 62 percent. According to the information provided by the contractor representative, the contractor has made progress in increasing its number of certified personnel. The contractor and the contracting officer should ensure that all of their personnel in IA positions at DTRA are certified.

## Central Repository of Certifications

The DTRA official responsible for overseeing DTRA's compliance with DOD 8570.01-M requirements did not maintain a central repository of all IA certifications. We requested supporting documentation that substantiated the FISMA submissions, but the DTRA official stated that DTRA did not maintain this information. During the course of the audit, the DTRA official began to collect copies of certifications. DTRA should maintain a central repository of all IA certifications to ensure that personnel have met the requirements. In addition, the repository will serve as support for future FISMA and DTRA IA Workforce Improvement Program reports.

### Tool for Identification and Tracking of IA Personnel

DTRA did not have an adequate tracking tool to identify personnel in the IA workforce or monitor whether they have obtained the appropriate certifications. During our initial visit in July 2009, a DTRA official provided us with an IA tracking spreadsheet that listed the DTRA IA workforce and the certifications they obtained. However, the official stated that the spreadsheet was unreliable and, in August 2009, stated that DTRA did not use it to answer the 2009 FISMA response. When we asked for documentation that supported the 2009 FISMA response, the official provided documents with highlights, crossed-out names, asterisks with no explanations, and hand-written annotations. We reviewed each item on the 2009 FISMA response with the official to identify the IA workforce and certifications and found many errors. By not having an adequate tracking tool to identify the IA workforce or the certifications that they obtained, DTRA incorrectly reported its IA workforce in the 2009 FISMA response. We believe that establishing and maintaining a tracking tool (for example, a database or spreadsheet) will help reduce the number of errors in DTRA's reporting of IA personnel and their certifications.

### *Inclusion of Clause in IA Contracts*

DTRA did not ensure that contracting officers added contract language requiring all IA contractor personnel to be certified to contracts for IA services. DFARS 239.7103(b) requires the use of the clause from DFARS 252.239-7001 in solicitations and contracts involving performance of IA functions. DTRA did not include the required DFARS clause in six of seven contracts we identified for IA services. Further, the DOD 8570.01-M requires that contract language must specify certification requirements as established by the manual, and that existing contracts must be modified at an appropriate time to include the requirements. The DFARS clause requires each contractor to ensure that contractor personnel have the appropriate baseline and computing environment certifications. In addition, the clause requires that personnel who do not have the appropriate certifications be denied access to DOD information systems. DTRA should include the appropriate DFARS clause in new contracts for performance of IA functions and should modify existing contracts to include this clause so that contractors are bound to these contractual requirements.

## Summary

DOD 8570.01-M establishes baseline IA technical and management skills among personnel performing IA functions across DOD. Further, DOD 8570.01-M attempts to provide a mechanism to verify IA workforce knowledge and skills through standard certification testing. DTRA personnel did not follow established guidance for identification and certification requirements of personnel having IA responsibilities. Specifically, DTRA did not meet certification requirements for IA personnel, did not properly report IA information to DOD in their 2009 FISMA response, and did not input IA information into the Defense Civilian Personnel Data System and the Defense Workforce Certification Application. These conditions occurred because DTRA did not adequately oversee its IA workforce. Specifically, DTRA did not have an adequate process in place to identify IA personnel and monitor whether IA personnel obtained the

appropriate certifications and did not ensure that contracting officers added contract language requiring all contractor personnel to be certified to contracts for IA services. As a result, DTRA's IA workforce may not have an adequate understanding of the concepts, principles, and applications of IA to enhance the protection and availability of DTRA's information systems and networks. Further, DOD and Congress did not have accurate information on DTRA's IA workforce and progress towards meeting milestones established by DOD 8570.01-M.

## Recommendations, Management Comments, and Our Response

**A.1. We recommend that the Director, Defense Threat Reduction Agency, develop and implement an adequate process to identify information assurance workforce personnel within the Defense Threat Reduction Agency and monitor whether the information assurance workforce obtains the appropriate certifications. Specifically the Director, Defense Threat Reduction Agency, should:**

**a. Establish an ongoing process through the use of designated points of contact to identify information assurance personnel and to monitor whether the information assurance personnel obtain the appropriate certifications.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will establish a process with designated personnel to identify information assurance personnel and will determine whether personnel obtained the appropriate certifications.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**b. Develop an adequate tool to identify and track the information assurance personnel.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will procure or develop a process to track the information assurance workforce.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**c. Track whether new civilian and military information assurance personnel obtain the appropriate certifications within 6 months of beginning work in an information assurance position.**

## *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will develop a tool to track information assurance personnel.

## *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**d. Ensure that contractors provide only certified information assurance personnel.**

## *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed and stated that the Designated Approving Authority issued a letter on January 6, 2010, directing a contractor to ensure that its information assurance workforce meet DOD 8570.01-M certification requirements within 6 months.

## *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**e. Maintain a central repository of certifications for information assurance personnel.**

## *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will maintain electronic and hard copy certifications of its information assurance workforce.

## *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**f. Enter the required information assurance position information into the Defense Civilian Personnel Data System.**

## *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency personnel will enter

the information assurance workforce data into the Defense Civilian Personnel Data System by October 1, 2010.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**g. Require information assurance personnel to authorize release of their certification information in the Defense Workforce Certification Application.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will require all information assurance personnel to authorize the release of their certification information in the Defense Workforce Certification Application.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**A.2. We recommend that the Director, Defense Threat Reduction Agency, include the clause in the Defense Federal Acquisition Regulation Supplement 252.239-7001 in new contracts for the performance of information assurance functions and modify existing contracts at an appropriate time to include the clause.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will include the clause in DFARS 252.239-7001 in new contracts and it will review and modify existing contracts where appropriate.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**A.3. We recommend that the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer modify DOD 8570.01-M to require all DOD information assurance personnel to authorize release of their certification information in the Defense Workforce Certification Application.**

### *Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer Comments*

The Acting Deputy Assistant Secretary of Defense (Identity and Information Assurance) in the Office of the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer agreed. The Acting Deputy Assistant

Secretary stated that the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer modified Change 2 of DOD 8570.01-M to include a requirement for the information assurance workforce to request release of their certification status to DOD through the Defense Workforce Certification Application.

## *Defense Threat Reduction Agency Comments*

Although not required to comment, the Director, Defense Threat Reduction Agency, agreed that the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer should modify DOD 8570.01-M to require all DOD information personnel to authorize release of their certification information in the Defense Workforce Certification Application.

## *Our Response*

The comments from the Acting Deputy Assistant Secretary of Defense (Identity and Information Assurance) are responsive, and the actions meet the intent of the recommendation.

# Finding B. Disabling of Accounts

DTRA did not disable information system accounts in a timely manner after personnel left the agency. Specifically, DTRA did not disable 17 accounts within 9 information systems and networks after personnel left the agency. Additionally, of 87 disabled accounts that we reviewed, 84 accounts remained active[*] more than 5 days after the personnel left the agency, and 66 accounts remained active more than 30 days. The accounts remained active because:

- system representatives for most DTRA systems reviewed were not notified when personnel left the agency and
- DTRA system administrators did not consistently review information system accounts that had not been used in a 30-day period.

Although we found no instances of unauthorized access after personnel left DTRA, the individuals could have accessed sensitive information within DTRA information systems and networks.

## Guidance for Disabling Accounts

DOD Instruction 8500.02 states that individual accounts designated as inactive, suspended, or terminated should be promptly deactivated.

The National Institute on Standards and Technology (NIST) issued Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3, August 2009, to provide guidance for recommended security controls for Federal information systems. NIST Special Publication 800-53 states that an organization should manage information system accounts by notifying account managers when temporary accounts are no longer required, information system users leave the agency or are transferred, or information system usage or user need-to-know changes. Further, NIST Special Publication 800-53 states that organizations should deactivate temporary accounts that are no longer required and deactivate accounts of users who leave the agency or are transferred.

DTRA issued its internal DTRA Directive 8500.01, "Defense Threat Reduction Agency (DTRA) Information Assurance (IA)," January 29, 2007, to establish policy, define roles and assign responsibilities to achieve IA within DTRA. DTRA Directive 8500.01 states that user accounts will be removed or reassigned within 2 days of notification that a user no longer requires access to the system. The Directive states that users and supervisors are responsible for notifying system administrators or IA officers when access is no longer required. Further, DTRA Directive 8500.01 states that system administrators will suspend user accounts and passwords that have not been used in a 30-day period.

---

[*] We consider information system accounts active if the ability to log into the system and access information has not been disabled.

## Disabling of Accounts

DTRA did not disable 17 accounts after personnel left the agency. Additionally, for some of the accounts that DTRA disabled, they did not do so in a timely manner.

### *Review of Active Accounts*

DTRA did not disable 17 accounts within 9 information systems and networks after personnel left the agency. We reviewed active accounts for 17 systems at DTRA including one mission-critical system, 15 mission-essential systems, and one mission-support system (see the Appendix for additional details on how we selected the DTRA systems for review). We found that 17 accounts within 9 of the 17 systems remained active after personnel had left the agency. Those 17 active accounts included accounts for civilian, military, and contractor personnel and visitors to DTRA. These accounts remained active for a period of 33 to 128 days, averaging 65 days, after the personnel had left the agency. Table 5 provides details of the active accounts we found for personnel who had left DTRA and the length of time since they had left.

**Table 5. Active Accounts for Personnel Who Left DTRA**

| System | Number of Active Accounts for Personnel that Departed | Days Active after Departure | Days Active after Departure (Average) |
|---|---|---|---|
| A | 1 | 48 | 48 |
| B | 5 | 35 – 128 | 60 |
| C | 2 | 36 – 56 | 46 |
| D | 1 | 37 | 37 |
| E | 3 | 85 – 97 | 91 |
| F | 1 | 90 | 90 |
| G | 1 | 97 | 97 |
| H | 2 | 34 – 105 | 70 |
| I | 1 | 33 | 33 |
| **Total** | **17** | **33 - 128** | **65*** |

*Average days for all 17 accounts rather than average for each of the systems.

### *Timeliness of Disabling of Accounts*

Of 87 disabled accounts that we reviewed, 84 accounts remained active 5 days after the personnel left the agency, and 66 accounts remained active for over 30 days. We attempted to obtain disabled account listings with the dates that the accounts were disabled for all 17 systems that we reviewed; however, we were only able to obtain 4 complete disabled account listings. We could not obtain listings for many of the systems because of system capabilities. We were able to review 87 accounts that were disabled on or after the date personnel left the agency for the 4 listings we received. The amount of time it took DTRA personnel to disable the accounts from when the personnel left DTRA ranged from 1 day to 1,392 days and averaged 455 days.

Table 6 provides details of the timeliness of disabling accounts for the four account listings we were able to review.

**Table 6. Timeliness of Disabling of Accounts**

| Days Before Accounts Were Disabled | # of Accounts |
|---|---|
| 0-5 Days | 3 |
| 6-10 Days | 7 |
| 10-30 Days | 11 |
| More than 30 Days | 66 |
| **Total** | **87** |

# Internal Controls Over Disabling Accounts

DTRA did not disable accounts in a prompt manner when personnel left their positions because:

- system representatives for most DTRA systems reviewed were not notified when personnel left the agency and
- DTRA system administrators did not consistently review information system accounts that had not been used in a 30-day period.

## *Notification of Personnel Departures*

System representatives were not always notified when personnel left DTRA. DTRA Directive 8500.01 states that users and supervisors are responsible for notifying system administrators or IA officers when access is no longer required. However, many accounts continued to be active well after personnel left the agency. DTRA uses an automatically generated e-mail to notify system personnel of the requirement to disable accounts. However, DTRA does not include representatives from all DTRA systems in the e-mail. Instead, this e-mail is sent only to those personnel who voluntarily request that DTRA include them in the e-mail distribution. DTRA includes representatives that oversee the DTRA networks in the e-mail, but did not include representatives from the majority of the other information systems that we reviewed. During discussions with representatives from some of the systems, they informed us that they have no way of knowing when personnel leave the agency other than word of mouth. The out-processing e-mail could be an effective control if expanded to include representatives from all DTRA information systems. DTRA should notify representatives from all DTRA information systems when personnel leave the agency.

## *Review of Inactive Accounts*

DTRA system administrators did not consistently review information system accounts that had not been used in a 30-day period. DTRA Directive 8500.01 states that system administrators should suspend user accounts and passwords that have not been used in a 30-day period. All 17 accounts that we identified as not disabled properly were active for more than 30 days after the personnel left the agency. Further, 66 of the 87 accounts

disabled by DTRA were active for more than 30 days after the personnel had left the agency. We understand that some accounts may need to remain active for specific reasons (for example, travel); however, this should be on an exception basis. DTRA should emphasize the importance of performing routine reviews of active accounts and suspending user accounts and passwords that have not been used in a 30-day period in accordance with DTRA guidance.

## Unauthorized Access to Sensitive Information

As a result of not notifying the appropriate system representatives and not having a process to identify inactive accounts, unauthorized individuals could have accessed sensitive information within DTRA information systems and networks. All of the systems we reviewed except one were reported as either mission-critical or mission-essential systems. Additionally, accounts for some systems containing classified information were not disabled promptly. However, we found no instances of unauthorized access for the active accounts we identified that should have been disabled. Maintaining proper account management procedures will help ensure the confidentiality and integrity of information in DTRA's information systems.

## Recommendations, Management Comments, and Our Response

**B. We recommend that the Director, Defense Threat Reduction Agency:**

**1. Notify system representatives for each of the Defense Threat Reduction Agency information systems when Defense Threat Reduction Agency personnel, contractors, or other visitors leave the agency.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency will provide system representatives with personnel departure dates. Further, he stated that the system representatives will develop procedures to ensure appropriate user account management and maintenance.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

**2. Establish a process to ensure that active accounts are reviewed at least monthly, and accounts and passwords that have not been used in a 30-day period are suspended for all systems in accordance with Defense Threat Reduction Agency guidance.**

### *Defense Threat Reduction Agency Comments*

The Director, Defense Threat Reduction Agency, agreed. The Director, Defense Threat Reduction Agency, stated that the Defense Threat Reduction Agency disabled all

accounts identified in the report. Further, he stated that the Defense Threat Reduction Agency will develop a monthly review process for disabling inactive accounts.

### *Our Response*

The Defense Threat Reduction Agency comments are responsive, and the actions meet the intent of the recommendation.

# Appendix. Scope and Methodology

We conducted this performance audit from June 2009 through February 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Review of the Information Assurance Workforce

We met with personnel from DTRA, the Defense-Wide Information Assurance Program from the Office of the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer, the Civilian Personnel Management Service, and the Defense Manpower Data Center.

We reviewed DOD Directive 8570.01 and DOD 8570.01-M. We also reviewed memoranda issued by the Director, Civilian Personnel Management Service and the Under Secretary of Defense for Personnel and Readiness on June 4, 2007, and August 27, 2008, respectively.

We reviewed DTRA's 2009 FISMA response, which identified DTRA's IA workforce and their certification status. We attempted to verify the response by reviewing supporting documentation; however, we found that DTRA did not maintain adequate documentation to support the response. With the assistance of the DTRA official responsible for compiling IA personnel data, we manually examined each number on the FISMA response and the supporting documentation. We attempted to verify certification information and identify additional IA personnel certifications by sending e-mails to the IA personnel originally identified by DTRA as performing IA functions, meeting with selected program managers, and meeting with contracting administrative personnel. We asked personnel to provide supporting documentation that showed that IA personnel obtained DOD-approved IA baseline certifications and computing environment certifications as required in DOD 8570.01-M.

We determined whether DTRA had entered IA workforce information into the Defense Civilian Personnel Data System. We also determined whether DTRA personnel had released their IA information using the Defense Workforce Certification Application.

## Disabling of Accounts

We met with personnel from DTRA and we reviewed DOD Directive 8500.01E and DOD Instruction 8500.02. We also reviewed NIST Special Publication 800-53 and DTRA Directive 8500.01.

We decided to review the most sensitive systems at DTRA. We selected 21 systems that DTRA reported as either mission-critical or mission-essential for our review. We also added one system that DTRA reported as mission-support; however, we believe that it

may have been reported incorrectly. During our first site visit, we determined from DTRA personnel that four of the systems we included were groups of hardware and software, such as routers, switches, repeaters, and intrusion detection services, used to enable the DTRA systems. Also we found that one system had been replaced by another system. The program manager for the systems told us that it was no longer in use. As a result, we included 17 systems in our review of disabling accounts.

We requested and obtained listings of all active accounts for each of the 17 systems. We also requested and obtained a listing of active and departed personnel with personnel that had departed as far back as November 2000. Additionally, we requested and obtained a listing of all personnel actions that related to personnel leaving the agency (for example, retirements, terminations, and resignations). We compared the listings to determine if the listings of active accounts included any personnel who had left the agency. We then determined how long the account had inappropriately been active based on the departure dates of the personnel. For the active accounts for personnel that had left the agency, we determined if unauthorized access was gained by the personnel after they departed by reviewing the last login dates, if available. We eliminated many entries in our results where personnel had departed as one category of personnel and came back as another and was still active under that other category (for example, military personnel left the agency and returned as contractors and were still current in their database). For the personnel who were listed as departing in multiple categories on different dates, we used the most recent date to compare to the account deletion dates (for example, military personnel who left the agency and returned as contractors and then left the agency at a later date).

We also requested disabled account listings with the dates that the accounts were disabled for each of the 17 systems reviewed. We received only four disabled account listings with disabled dates that we could use for our review mainly because of system constraints. For those four systems, we compared the disabled accounts listings to the active and departed personnel listing to determine the length of time the accounts remained active prior to being disabled. However, we excluded the following types of accounts from our review because we could not determine when the account should have been disabled:

- personnel who still worked at DTRA in any capacity,
- personnel who left DTRA after the disabled date, and
- personnel who we could not match to the active and departed personnel listing.

For the personnel who were listed as departing in multiple categories on different dates, we used the most recent date to compare to the account deletion dates. As a result, we were able to review 87 accounts within the 4 systems.

## Use of Computer-Processed Data

We did not use computer-processed data to determine whether personnel obtained the appropriate certifications. Instead, for those personnel identified by DTRA personnel as part of the IA workforce, we obtained electronic and hard-copy supporting documentation that indicated personnel obtained the appropriate certifications.

We relied on data from DTRA's Secure Access database that includes information on all current and departed personnel. The Secure Access database identifies the departure date of those personnel who have left the agency, which we used in our analysis of whether DTRA disabled accounts in a timely manner. We did not rely on the departure dates for our analysis of active accounts within DTRA systems because we verified the departure dates through obtaining other supporting documentation. However, we relied on the departure dates in the Secure Access database for our analysis on determining whether disabled accounts were disabled in a timely manner for personnel. We selected a judgmental sample for the 87 accounts reviewed and requested supporting documentation for the sample of accounts to verify the personnel departure dates. The supporting documentation validated the departure dates for the accounts we selected. As a result, we believe we can sufficiently rely on the departure dates in the Secure Access database for our analysis.

## Prior Coverage

No prior audit coverage has been conducted over the last 5 years on certification of IA personnel or disabling of accounts at the Defense Threat Reduction Agency. However, the Government Accountability Office (GAO) has issued one report discussing controls over the identification of IA personnel within Defense agencies. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov.

### *GAO*

GAO Report No. GAO-07-528, "Information Security - Selected Departments Need to Address Challenges in Implementing Statutory Requirements," August 2007

# Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NETWORKS AND
INFORMATION
INTEGRATION

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: AUDITING; READINESS, OPERATIONS AND
SUPPORT)

SUBJECT: Selected Controls for Information Assurance at the Defense Threat Reduction Agency Project Number: D2009-D000LB-0216.000 dated February 16, 2010

This is in response to Draft Report (attached) dated February 16, 2010, requesting comments on the findings and recommendations contained in the draft report.

ASD(NII)/DoD CIO concurs and has incorporated into Change 2 of the DoD 8570.01-M, which is currently being staffed (NII000192-10), the requirement for certified IA Workforce Members to request release of their certification status to the DoD via the Defense Workforce Certification Application (DWCA). We expect Change 2 to the DoD 8570.01-M to be published by April 30, 2010.

Thank you for the opportunity to comment on the draft report.

Gary D. Guissanie
Acting Deputy Assistant Secretary of Defense
(Information and Identity Assurance)

Attachments:
As stated

# Defense Threat Reduction Agency Comments

Defense Threat Reduction Agency
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201

MAR 2 6 2010

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Defense Threat Reduction Agency (DTRA) Response to the Discussion Draft of a Proposed Report, Project No. D2009-D000LB-0216.000, "Selected Controls for Information Assurance at the Defense Threat Reduction Agency"

Thank you for the opportunity to expand our response dated March 22, 2010, to the subject report regarding DTRA's information assurance controls. Our expanded responses assign completion dates for each recommendation and clarifies our previous submission. As stated in our first response, the Chief Information Officer is in the process of documenting policy, processes, and procedures related to information assurance. As that documentation is completed, we will provide your office copies.

My point of contact for this action is [redacted]

Kenneth A. Myers
Director

Attachment:
As stated

DTRA ACTIONS TO ADDRESS RECOMMENDATIONS IN DoD IG REPORT
PROJECT NO. D2009-D000LB-0216.000

Recommendation A.1: Information Assurance Workforce Personnel

DTRA Actions:

A.1.a. Concur. DTRA will implement a process and designate personnel to properly identify the information assurance workforce. DTRA's Chief Information Officer, in conjunction with DTRA's Human Capital Office and Agency program managers, will identify information assurance technical and managerial positions by May 15, 2010. DTRA will review the applicability of personnel certifications against their appropriate Information Assurance Technical level and their Information Assurance Management level. These actions will be completed as we update position descriptions during the National Security Personnel System (NSPS) transition to the General Schedule (GS) System on June 6, 2010.

A.1.b. Concur. DTRA will procure or develop a tool/process to track information assurance personnel. This action will be completed by August 1, 2010.

A.1.c. Concur. DTRA will initially develop a Microsoft SharePoint site as a tool to track those identified as members of the IA workforce. This will be completed by August 1, 2010.

A.1.d. Concur. DTRA issued a Designated Approving Authority letter on January 6, 2010, to the Information Technology Support Services performer directing them to achieve compliance with DoD 8570.01-M, "Information Assurance Training, Certification, and Workforce Management," information assurance workforce certification requirements within 6 months.

A.1.e. Concur. DTRA will maintain certifications within the Microsoft SharePoint site and as hard copy within the information assurance program managers' office. This action will be completed by August 1, 2010.

A.1.f. Concur. DTRA will enter the information assurance workforce information into Defense Civilian Personnel Data System (DCPDS). DTRA's Chief Information Officer, in conjunction with DTRA's Human Capital Office and Agency program managers, will identify information assurance technical and managerial positions by May 15, 2010. DTRA will use DoD 8570.01 and the DoD 8570.01 Frequently Asked Questions (FAQ) guidance on identification of information assurance workforce personnel. This data will be input into DCPDS by October 1, 2010.

A.1.g. Concur. DTRA will require that all personnel in an information assurance workforce position authorize the release of their certification information using the Defense Workforce Certification Application. This action will be completed by August 1, 2010.

Recommendation A.2: Use of DFAR Supplement 252.239-7001 in New and Existing Contracts

DTRA Actions: Concur. DTRA will include the required Defense Federal Acquisition Regulation Supplement clause 252.239-7001 in new contracts. For existing contracts, DTRA will scrutinize them for information assurance workforce applicability and modify as required. These actions will be completed within 90 days of identification of a contract with information assurance roles and responsibilities.

Recommendation A.3: Recommendation for ASD/NII/CIO to Modify DoD 8570.01-M.

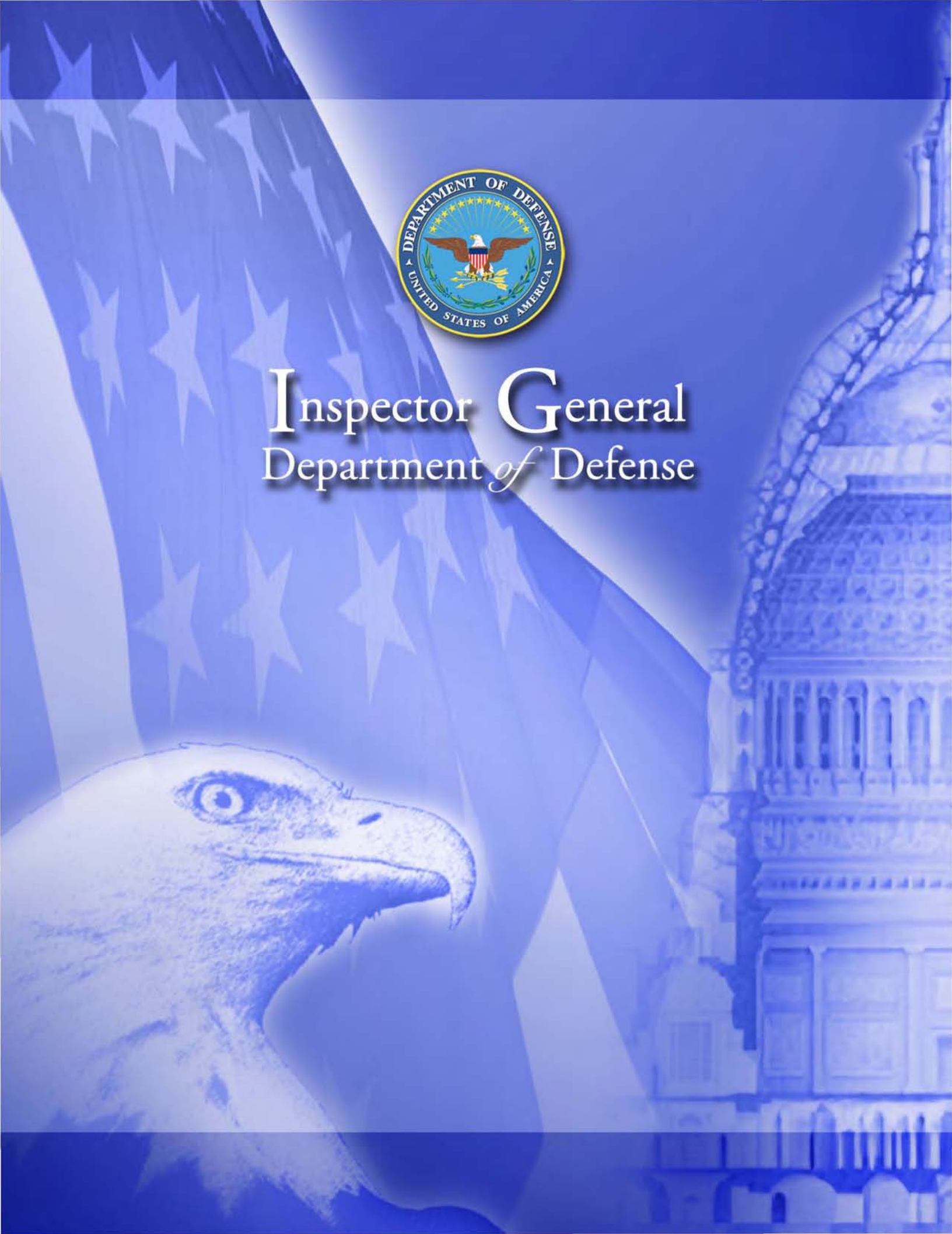
DTRA Comment: Concur; however, DTRA cannot affect this change. No action required by DTRA for this recommendation.

Recommendation B.1: Notification to System Representatives Regarding Departure of Personnel

DTRA Actions: Concur. DTRA will notify system owners of departure dates of personnel. This action will be completed by April 30, 2010. In addition, DTRA systems owners and representatives will develop work instructions to ensure the proper management and maintenance of user accounts. This action will be completed by April 30, 2010.

Recommendation B.2: Establish Monthly Review Process

DTRA Actions: Concur. Accounts that were identified by the DoD IG were disabled. DTRA will develop work instructions for the disabling of accounts and will establish a monthly review process. This action will be completed by April 30, 2010. Until then, accounts are disabled on "Date Eligible for Return From Overseas" or when an employee terminates employment at DTRA. The DTRA Senior Information Assurance Officer will conduct periodic checks to ensure the accounts are disabled.


Inspector General
Department of Defense