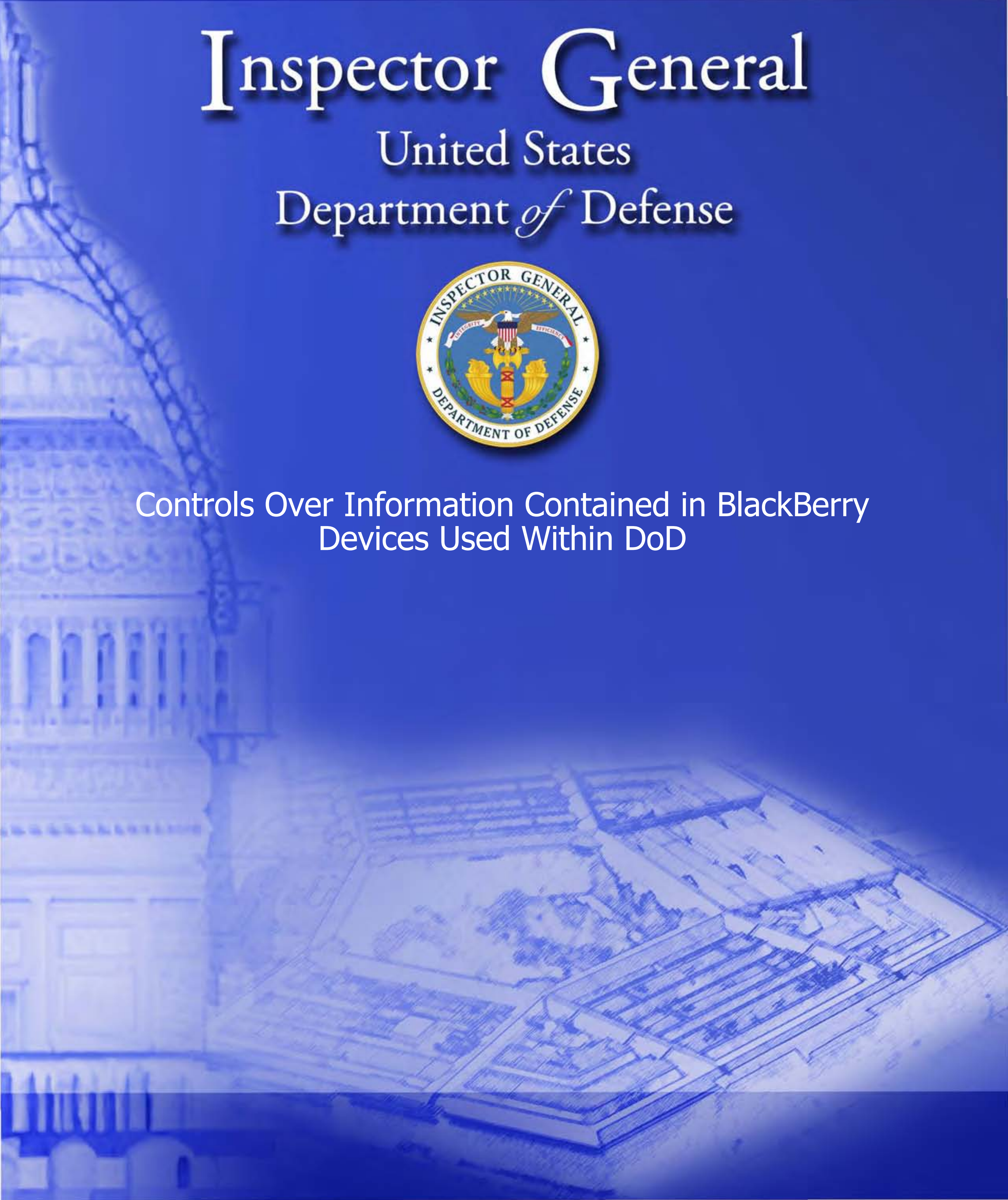
Report No. D-2009-111 September 25, 2009

Inspector General

United States

Department of Defense

Controls Over Information Contained in BlackBerry Devices Used Within DoD



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

DEPARTMENT OF DEFENSE
hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

Acronyms and Abbreviations

AIM	Asset Inventory Management
ASD(NII)/DoD CIO	Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer
BES	BlackBerry Enterprise Server
CIO	Chief Information Officer
CTO	Communications Tasking Order
DCMA	Defense Contract Management Agency
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
JTF-GNO	Joint Task Force-Global Network Operations
PDA	Personal Digital Assistant

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

September 25, 2009

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)

SUBJECT: Controls Over Information Contained in BlackBerry Devices Used Within DoD (Report No. D-2009-111)

We are providing this report for your review and comment. We considered management comments on a draft of this report when preparing the final report. The complete text of the comments is in the Management Comments section of the report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer comments on Recommendations 1.a and 1.b are not responsive and the comments on Recommendations 1.c through 1.f are partially responsive. Therefore, we request revised comments on Recommendations 1.a through 1.f by October 25, 2009. The Air Force Chief Information Officer did not provide comments prior to issuance of the final report; therefore, we request comments on Recommendations 2.a through 2.c by October 25, 2009.

If possible, send a .pdf file containing your comments to audros@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8905 (DSN 664-8905).

Paul J Granetto

Paul J. Granetto
Assistant Inspector General
Readiness, Operations, and Support

Report No. D-2009-111 (Project No. D2008-D000LC-0131.000) September 25, 2009

Results in Brief: Controls Over Information Contained in BlackBerry Devices Used Within DoD

What We Did

Our objective was to determine whether the Military Services and other Defense agencies have controls in place to prevent unauthorized disclosure of information contained in wireless devices. Specifically, we reviewed controls to protect information contained in BlackBerry devices as these are the primary Personal Digital Assistant (PDA) devices used by the Military Services and other Defense agencies. We visited various Air Force, Defense Contract Management Agency (DCMA), Defense Information Systems Agency, and Defense Logistics Agency locations to assess their controls over BlackBerry devices. We also reviewed DoD criteria governing BlackBerry devices.

What We Found

DoD Components did not always implement adequate controls to properly secure information on BlackBerry devices. For example,

- passwords did not always meet the length and complexity requirements of DoD Instruction 8500.2;
- the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer (ASD[NII]/DoD CIO) allowed DoD Components to use their discretion in not implementing required controls, such as encrypting data stored on BlackBerry devices, properly implementing user agreements, and requiring passwords to expire and devices to lock out after a specified period of time; and
- annual information assurance training did not always include wireless topics in accordance with DoD Directive 8100.02.

What We Recommend

We recommend that the ASD(NII)/DoD CIO:

- revise the DoD BlackBerry Security Checklist to require all DoD BlackBerry device passwords to, at a minimum, comply with DoD Instruction 8500.2 and develop a written plan to implement the use of two-factor authentication;
- ensure that the correct risk levels are assigned to all BlackBerry security controls and ensure that only high and medium risk levels are designated as “required” and
- clarify the specific wireless topics required in annual information assurance training.

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

- reconcile the PDA password requirements in Air Force Instruction 33-200.
- implement controls to ensure PDA inventory transactions are recorded in the official inventory system
- ensure all security settings are validated and a written authority to operate is issued for the BlackBerry Enterprise Server that services Andrews and Bolling Air Force Bases.

Management Comments and Our Response

The ASD(NII)/DoD CIO comments were partially responsive. DCMA provided comments on the Finding and recommendations. We did not receive comments from the Air Force CIO prior to issuance of the final report. We request that the ASD(NII)/DoD CIO provide revised comments on the final report by October 25, 2009 and that the Air Force CIO also provide comments by October 25, 2009. Please see the recommendations table on page ii.

Report No. D-2009-111 (Project No. D2008-D000LC-0131.000) September 25, 2009

Recommendations Table

Management	**Recommendations Requiring Comment**	**No Additional Comments Required**
Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer	1.a, 1.b, 1.c, 1.d, 1.e, and 1.f	
Air Force Chief Information Officer	2.a, 2.b, and 2.c	

Please provide comments by October 25, 2009.

Table of Contents

Introduction

Objectives

The overall objective of the audit was to determine whether the Military Services and other Defense agencies have controls in place to prevent unauthorized disclosure of information contained in wireless devices. Specifically, we reviewed controls to protect information contained in BlackBerry devices as these are the primary Personal Digital Assistant (PDA) devices used by the Military Services and other Defense agencies. See Appendix A for the scope and methodology and prior audit coverage.

Background

PDAs are small, portable electronic devices with similar functional use as a personal computer with the convenience of portability. However, with the convenience of portability comes the risk of loss, which could lead to the compromise of DoD information. Therefore, DoD Components must implement proper security controls to prevent unauthorized disclosure.

A BlackBerry device incorporates features, such as an organizer (address book, calendar, and to-do lists) and instant messaging with wireless services, such as e-mail, mobile telephone, and web browsing. The use of BlackBerry devices is prevalent among high-level officials such as senior management, personnel requiring access to DoD information technology resources during non duty hours, and personnel who are frequently separated from the office. Because BlackBerry devices can introduce security vulnerabilities exposing Government information systems to compromise, BlackBerry devices must be properly secured.

The BlackBerry Enterprise Server (BES) permits a DoD-compliant information system Security policy to be enforced on all BlackBerry devices. The BES provides a centralized link between BlackBerry devices, BlackBerry applications, and wireless networks, while integrating devices into an organization’s e-mail system.

Criteria Governing BlackBerry Devices

DoD Directive 8100.02, “Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),” April 14, 2004, provides policy and responsibilities for the security of commercial wireless devices used throughout DoD. The Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer (ASD[NII]/DoD CIO) is responsible for developing DoD wireless policy.

The Defense Information Systems Agency (DISA) issued the, “DoD Wireless Security Technical Implementation Guide, DISA Version 5, Release 2,” November 15, 2007 (DoD Wireless Security Technical Implementation Guide), to implement DoD 8100.02.

DISA also issued the, “DoD Wireless Security Technical Implementation Guide, BlackBerry Security Checklist, Version 5, Release 2.1,” November 15, 2007, (November 2007 DoD BlackBerry Security Checklist) to provide minimum baseline BlackBerry security guidance for DoD. DISA also updated the November 2007 DoD BlackBerry Security Checklist and issued the, “DoD Wireless Security Technical Implementation Guide, BlackBerry Security Checklist, Version 5, Release 2.2,” September 15, 2008 (September 2008 DoD BlackBerry Security Checklist). The DoD Wireless Security Technical Implementation Guide and BlackBerry Security Checklist outlines the responsibilities of the Designated Approving Authority [1] as well as the following standards related to the protection of information on BlackBerry devices:

- password protection for BlackBerry devices,
- encryption of data stored on BlackBerry devices,
- signed user agreements for BlackBerry devices,
- inventory records of BlackBerry devices, and
- physical security of the BES.

On June 5, 2008, the Joint Task Force-Global Network Operations (JTF-GNO)[2] issued Communications Tasking Order (CTO) 08-009, “Implementation Timelines for Encryption of Sensitive Unclassified Data-at-Rest (DAR) within the DoD,” establishing “data-at-rest” encryption instructions and milestones for reporting encryption status. Data-at-rest encryption is the encryption of information stored on hard drives to prevent unauthorized access to that information.

BlackBerry Devices Used in DoD

As of January 2008, DoD Components reported approximately 63,000 BlackBerry devices used within DoD that have the ability to process sensitive information. The Air Force, Defense Contract Management Agency (DCMA), DISA, and Defense Logistics Agency (DLA) accounted for over 55 percent (34,961) of the BlackBerry devices reported to DoD. Table 1 shows the number of BlackBerry devices reported by Air Force, DCMA, DISA, and DLA.

[1] The Designated Approving Authority has the authority to assume responsibility for operating an information system at an acceptable level of risk. Once the Designated Approving Authority deems the level of risk to be acceptable, they grant the system authority to operate.

[2] The Director of DISA is also the commander of JTF-GNO and is responsible for directing the operation and defense of the DoD network.

Table 1. Devices Reported by Air Force, DCMA, DISA, and DLA in January 2008	
DoD Components	**Number of Devices**
Air Force	30,000
DCMA	3,000
DISA	793
DLA	1,168
Total	**34,961**

We reviewed BlackBerry controls at the Air Force, DCMA, DISA, and DLA.

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 the DoD. Specifically, DoD did not always implement adequate controls to properly secure information on BlackBerry devices. See the Finding paragraph for more detailed explanation. Implementing Recommendations 1.a.-f. and 2.a.-c. should correct the internal control weaknesses identified in the report. We will provide a copy of this report to the senior officials responsible for internal controls in the ASD(NII)/DoD CIO, the Air Force, DCMA, DISA and DLA.

Finding. DoD BlackBerry Requirements

DoD Components did not always implement adequate controls to properly secure information on BlackBerry devices. Specifically:

- passwords did not always meet the length and complexity requirements of DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003;
- ASD(NII)/DoD CIO allowed DoD Components to use their discretion in not implementing required controls, such as encrypting (turning data into an unintelligible form) data stored on BlackBerry devices, properly implementing user agreements, and requiring passwords to expire and devices to lock out after a specified period of time;
- annual information assurance training did not always include wireless topics, nor was it clear what wireless topics should have been included in the annual information assurance training; and
- Air Force official inventory levels did not always reflect individual site inventory levels.

DoD Components did not always implement adequate controls because DoD issued conflicting guidance. In addition, Air Force did not always perform adequate oversight in regard to BlackBerry inventory levels. As a result, DoD cannot ensure that information contained in BlackBerry devices is adequately protected against unauthorized access.

Password Requirements

Passwords did not always meet the length and complexity requirements of DoD Instruction 8500.2. Specifically, Instruction 8500.2 states that DoD information systems[3] are accessed through the use of an individual identifier (for example, a user name) and a password. When a user login identifier is used with a password to access a system processing sensitive information, Instruction 8500.2 requires the password to be at least eight characters including at least one upper case letter, one lower case letter, one number, and one special character. Because a BlackBerry device can contain sensitive information and just a password can provide access to the information in the BlackBerry device, a BlackBerry device password should, at a minimum, follow the length and complexity requirements of DoD Instruction 8500.2. The Air Force, DCMA, DISA, and DLA sites that we visited did not always implement passwords in accordance with DoD requirements to protect sensitive information. For example, when we began the audit, the BESs at Andrews and Bolling Air Force Bases, DCMA, and DLA Headquarters were set

[3] DoD Instruction 8500.2 defines an information system as a set of information resources organized for collection, storage, processing, maintenance, use, dissemination, disposition, display, or transmission of information.

to enforce only passwords that were at least five characters,[4] as opposed to at least eight characters as required by DoD Instruction 8500.2. In addition, the BESs at DISA and Wright-Patterson Air Force Base were set to enforce passwords that were at least six characters and eight characters, respectively. However, with the exception of Andrews and Bolling Air Force Bases, none of the BESs at the sites we visited were set to enforce passwords that contained at least one uppercase letter, one lowercase letter, one number, and one special character.

DoD BlackBerry password requirements in the September 2008 DoD BlackBerry Security Checklist conflicted with the password requirements in DoD Instruction 8500.2. Even though BlackBerry devices can contain sensitive information, the September 2008 DoD BlackBerry Security Checklist permits the minimum BlackBerry device password to be only five characters, consisting of at least one letter and one number.

The DoD Wireless Security Technical Implementation Guide states that it creates an environment that meets DoD security requirements for protecting sensitive information, but its minimum BlackBerry password requirements do not meet DoD security requirements.

Air Force Chief Information Officer Password Guidance

The Air Force Chief Information Officer (CIO) issued unclear guidance regarding password requirements for PDAs. Specifically, Air Force Instruction 33-200, "Information Assurance (IA) Management," December 23, 2008, directs PDA users to the following three sets of guidance, each having different password requirements.

- DISA Wireless Security Technical Implementation Guide requires PDA passwords to be at least five characters.
- DISA Secure Remote Computing Security Technical Implementation Guide refers to password requirements in DoD Instruction 8500.2, which requires passwords to be at least eight characters with at least one upper case letter, one lower case letter, one number, and one special character for access to information systems processing sensitive information.[5]
- Air Force Manual 33-223, "Identification and Authentication," requires Air Force passwords to be at least nine characters with at least two upper case letters, two lower case letters, two numbers, and two special characters.

The different publications with different password requirements can create confusion among Air Force personnel regarding which password requirements they should follow

[4] The BES at Andrews and Bolling Air Force Bases was also set to require passwords for four BlackBerry devices to be at least eight characters.

[5] The DISA Secure Remote Computing Security Technical Implementation Guide requires PDA users who are not performing system administration functions to secure the PDA by following, to the fullest extent possible, the password requirements in DoD Instruction 8500.2.

for PDAs. This could lead to users not protecting information on PDAs to the extent intended by the Air Force CIO. The Air Force CIO should reconcile the various PDA password requirements in Air Force Instruction 33-200 to determine specific password requirements that PDA users must follow and adjust Air Force Instruction 33-200 accordingly.

Access Control Within DoD

ASD(NII)/DoD CIO representatives acknowledged that they would prefer to use two-factor authentication, such as a Common Access Card with a Personal Identification Number or a Common Access Card with biometrics, such as a finger print scan to access BlackBerry devices. Although the representatives stated they were not aware of any viable commercial versions of these technologies for BlackBerry devices, DoD Security Technical Implementation Guide, "Access Control in Support of Information Systems," Version 2, Release 2, December 26, 2008, requires two-factor authentication to access information systems processing sensitive information. In addition, DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008, states that the ASD(NII)/DoD CIO must ensure that biometrics are developed for access control and effectively integrated into information assurance efforts. However, the ASD(NII)/DoD CIO representatives said they had no written plan with milestones to implement two-factor authentication for accessing information in BlackBerry devices.

Because BlackBerry devices are mobile computing devices that can contain sensitive information, ASD(NII)/DoD CIO should revise the DoD BlackBerry Security Checklist to, at a minimum, require all DoD BlackBerry devices to have a password at least eight characters, including one upper case letter, one lower case letter, one number, and one special character in compliance with DoD Instruction 8500.2. In addition, ASD(NII)/DoD CIO should develop a written plan to implement the use of two-factor authentication for accessing information on BlackBerry devices.

Discretion in Implementing Controls

ASD(NII)/DoD CIO allowed DoD Components to use their discretion in not implementing required controls, such as encrypting data stored on BlackBerry devices; properly implementing user agreements; and requiring passwords to expire and devices to lock out after a specified period of time. The September 2008 DoD BlackBerry Security Checklist designated mandatory controls as "required" and discretionary controls as "optional." In addition, the September 2008 DoD BlackBerry Security Checklist also assigned a risk level to each control to indicate the risk to BlackBerry security when an organization does not implement the control. These risk levels relate to DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, which permits a Designated Approving Authority to approve a system to operate without correcting security weaknesses with low risk.[6] However, a Designated Approving Authority must satisfactorily mitigate a security weakness with medium risk and must not approve a system to operate without correcting security weaknesses with high risk. The September 2008 DoD BlackBerry Security Checklist designated some low risk controls as "required," which permitted the Designated Approving Authority to approve the system to operate without implementing some "required" controls. For example, Air Force and DCMA did not always implement "required" controls that were assigned a low level of risk.

Conflicting Guidance

ASD(NII)/DoD CIO officials did not fully reconcile requirements from the September 2008 DoD BlackBerry Security Checklist to risk levels in DoD Instruction 8510.01. According to DISA representatives, the intent of the September 2008 DoD BlackBerry Security Checklist was for DoD Components to implement all "required" security settings; however, according to the September 2008 DoD BlackBerry Security Checklist, some "required" controls were designated as low risk. As a result, the Designated Approving Authority could use discretion on whether or not to implement these controls. The ASD(NII)/DoD CIO should ensure that the correct risk levels are assigned to all BlackBerry security controls. For example, data-at-rest encryption is assigned a low level of risk; however, this control can prevent unauthorized access to information, which is more consistent with a higher level of risk. In addition, DISA assigned a low level of risk to the user agreement and no longer requires the seven topics; however the November 2007 BlackBerry Security Checklist assigned a medium level of risk to this control and ASD(NII)/DoD CIO representatives said the user agreement control should not be assigned a low level of risk. As a result, as part of the review of risk levels assigned to all BlackBerry controls, ASD(NII)/DoD CIO should assign a higher risk level to the data-at-rest encryption and user agreement controls and also require that the seven topics be included in user agreements. After ensuring that the correct risk levels have been assigned to all BlackBerry controls, ASD(NII)/DoD CIO should then ensure that only high and medium risk controls are designated as "required" and ensure that controls identified as low risk are not designated as "required." Once ASD(NII)/DoD CIO resolves these issues within the DoD BlackBerry Security Checklist, DoD Components should review their controls to ensure they have fully met established requirements.

Encryption Requirements

Air Force and DCMA did not always encrypt data stored on BlackBerry devices. Specifically, Andrews, Bolling, and Wright-Patterson Air Force Bases and DCMA did not encrypt data stored on their BlackBerry devices, which was a "required" control in the November 2007 DoD BlackBerry Security Checklist. The November 2007 DoD BlackBerry Security Checklist states that information assurance officers must ensure that

[6] DoD Instruction 8510.01 designates risk levels using severity categories of I, II, or III with severity category I designating the greatest risk level. For this audit report, we use the term high risk to represent severity category I, medium risk to represent severity category II, and low risk to represent severity category III.

they encrypt all data stored on the BlackBerry devices. In addition, the JTF-GNO CTO 08-009 states that all DoD Components must meet specific milestones for encrypting the data stored in their BlackBerry devices in accordance with the November 2007 DoD BlackBerry Security Checklist, which assigned a low level of risk to this "required" control.

User Agreements

DCMA did not properly educate BlackBerry users on their roles and responsibilities when using the BlackBerry device. Specifically, the November 2007 DoD BlackBerry Security Checklist requires that information assurance officials develop a user agreement between the component and BlackBerry users. The November 2007 DoD BlackBerry Security Checklist states that officials should have users of BlackBerry devices read and acknowledge that they have accepted their roles and responsibilities regarding safeguarding information on BlackBerry devices. The user agreement must include the following seven topics:

1. type of access required by the user;
2. responsibilities, liabilities, and security measures involved in the use of the BlackBerry device;
3. incident handling and reporting procedures along with a designated point of contact;
4. responsibility for damage caused to a Government system or data through negligence or a willful act;
5. general security requirements and practices;
6. for classified devices, user responsibility to adhere to DoD policy in regard to facility clearances, protection, storage, distribution, etc.; and
7. Government-owned hardware and software is used for official duties only, where the employee is the only individual authorized to use the device.

Although the November 2007 BlackBerry Security Checklist assigned a medium level of risk to the user agreement requirement, the September 2008 DoD BlackBerry Security Checklist assigned a low level of risk to the requirement. In April 2009, DISA revised the DoD BlackBerry Security Checklist to recommend but no longer require the seven topics to be in the user agreement.

Password Expiration and Device Lock Out Requirements

Andrews and Bolling Air Force Bases and DCMA did not always configure their BESs to require BlackBerry device passwords to expire after a specified period of time. In addition, Air Force and DCMA did not always configure their BESs to require

BlackBerry devices to lock out after a specified period of time.[7] Specifically, the September 2008 DoD BlackBerry Security Checklist requires that BlackBerry users change their passwords every 90 days and requires BlackBerry devices to lock out after 60 minutes, regardless of activity or inactivity. However, the September 2008 DoD BlackBerry Security Checklist assigned a low level of risk to the requirements.

Annual Information Assurance Training

Annual information assurance training did not always include wireless topics, nor was it clear what wireless topics should have been included in the annual information assurance training. DoD Directive 8100.02 directs the heads of DoD Components to ensure the Designated Approving Authority incorporates wireless topics in annual information assurance training. However, Andrews, Bolling, and Wright-Patterson Air Force Bases and DCMA did not include wireless topics in their annual information assurance training. Although DISA and DLA annual information assurance training included some wireless topics, we are not certain that the training met the requirements of DoD Directive 8100.02 because ASD(NII)/DoD CIO did not clarify the specific wireless topics that should be included in the training.

As a result, DoD cannot be certain that wireless users are fully aware of security risks associated with wireless devices such as BlackBerry devices. Therefore, ASD(NII)/DoD CIO needs to clarify the specific wireless topics required by DoD Directive 8100.02 and establish controls to help ensure that DoD wireless users receive annual information assurance training that includes these required wireless topics.

BlackBerry Devices Inventory

Component official inventory levels did not reflect individual site inventory levels. Specifically, the Andrews, Bolling, and Wright-Patterson Air Force Bases official BlackBerry inventory levels in the Asset Inventory Management (AIM) System, did not reflect the local base inventory levels. Air Force Instruction 33-112, “Information Technology Hardware Asset Management,” April 7, 2006, requires the Information Technology Asset Group to account for BlackBerry devices in the AIM System for their official property records. According to the AIM system; Andrews, Bolling, and Wright-Patterson Air Force Bases had a total of 1,589 BlackBerry devices.

[7] During the audit, Andrews and Bolling Air Force Bases configured their BES to require BlackBerry devices to lock out after a specified period of time. Although Wright Patterson Air Force Base did not configure their BES to require BlackBerry devices to lock after a specified period of time, they plan to implement this configuration.

However, the Andrews, Bolling, and Wright-Patterson Air Force Bases' local inventory records showed that they had a total of 2,861 BlackBerry devices in use. Table 2 shows the difference between inventory records at Andrews, Bolling, and Wright-Patterson Air Force Bases.

Table 2. Air Force BlackBerry Inventories

Air Force Base Location	Air Force AIM System Records	Air Force Bases' Local Inventory Records	Difference
Andrews[1]	34	233	199
Bolling[1]	102	292	190
Wright Patterson[2]	1,453	2,336	883
Total	**1,589**	**2,861**	**1,272**

[1] AIM and local inventory BlackBerry records as of May 2008.

[2] AIM and local inventory BlackBerry records as of July 2008.

The official inventory records did not reflect the individual site records because there was a lack of communication between the Andrews, Bolling, and Wright-Patterson Air Force Bases staff that maintained and configured their BlackBerry devices and the staff that managed their information technology assets. Although we reviewed only the inventory records for Andrews, Bolling, and Wright-Patterson Air Force Bases, this issue could be systemic because the Air Force instruction applies to the entire Air Force.

As a result of questionable inventory records within the Air Force, we cannot be certain that the Air Force reported an accurate number of BlackBerry devices with encryption as requested by JTF–GNO. In response to the January 2008 DoD data call, the Air Force reported 30,000 BlackBerry devices to ASD(NII)/DoD CIO; however, the AIM System showed only 14,566 BlackBerry devices in use by the Air Force as of April 2008. According to Air Force officials, the Air Force based the 30,000 BlackBerry device count on sales data from the manufacturer of the BlackBerry device versus the number of devices in their AIM System. Therefore, we cannot be certain that the 30,000 or the 14,566 is the total amount of BlackBerry devices in use by the Air Force. The Air Force should implement controls to ensure all transactions that affect the inventory of BlackBerry devices are recorded in their AIM System, and then use the system to accurately respond to official data calls such as the encryption data call from the ASD(NII)/DoD CIO in 2008.

Actions Taken During the Audit

During the audit, Andrews, Bolling, and Wright-Patterson Air Force Bases took steps to implement the BES configurations for encryption. We verified that Andrews and Bolling Air Force Bases configured the BES to encrypt data stored on BlackBerry devices. However, Wright-Patterson elected not to activate the setting that specifies the level of encryption on external files systems. Even though the Air Force took steps to encrypt data stored on their BlackBerry devices, the Designated Approving Authority for Andrews and Bolling Air Force Bases had not completed testing to validate all security settings and had not yet issued a written authority to operate. Therefore, the Designated Approving Authority for Andrews and Bolling Air Force Bases should validate all security settings and issue a written authority to operate. DCMA also took steps to encrypt data stored on BlackBerry devices by enabling the content protection feature on their BESs. However, DCMA excluded the address book from content protection. Andrews, Bolling, and Wright-Patterson Air Force Bases and DCMA also took steps to implement the BES configurations for password requirements. For example, both DCMA and the Air Force configured the passwords to expire in 90 days or less in accordance with the DoD BlackBerry Security Checklist.

Conclusion

As a result of unclear guidance from DoD and inadequate oversight by DoD Components, DoD cannot ensure information contained in BlackBerry devices is adequately protected from unauthorized access. The lack of clear guidance created confusion regarding whether DoD Components had to implement mandatory DoD controls. If DoD Components do not implement these mandatory controls, sensitive information on BlackBerry devices is more vulnerable to unauthorized disclosure and exploitation because of the BlackBerry device’s portability and the requirement of only a password to gain access. Therefore, DoD should ensure that information contained in BlackBerry devices is adequately protected against unauthorized access.

Recommendations, Management Comments, and Our Response

Defense Contract Management Agency Comments and our Response

Although DCMA was not required to comment, summaries of their management comments and our response are in Appendix B.

Comments on the Report

The Principal Director, Deputy Assistant Secretary of Defense for Cyber, Information, and Identity Assurance (the Principal Director) provided comments on the draft audit report for the DoD ASD(NII)/DoD CIO. Because the Principal Director references his comments to support his comments on Recommendation 1.a, we integrated the comments under Recommendation 1.a.

1. We recommend that the DoD Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer:

a. Revise the DoD BlackBerry Security Checklist to, at a minimum, require all DoD BlackBerry devices to have a password that is at least eight characters, including one upper case letter, one lower case letter, one number, and one special character in compliance with DoD Instruction 8500.2.

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

Although the Principal Director agreed that there should be a uniform length and complexity requirement for passwords for BlackBerry devices throughout the DoD, the Principal Director stated that password guidance for information systems in DoD Instruction 8500.2 does not directly apply to BlackBerry devices. Specifically, the Principal Director said that BlackBerry devices are not a “full-fledged” DoD information system because BlackBerry devices:

- operate on commercial wireless carriers that are not attached to the DoD network,
- store and process only unclassified DoD data,
- provide no direct network connection,
- provide no access to network resources,
- provide no network log-on capability,
- receive wireless communications encrypted at the BES, and
- are not considered physical nodes on the Global Information Grid.

In addition, the Principal Director stated that when the original Security Technical Implementation Guide was published in 2005, no DoD policy specified password length and complexity requirements for devices that stored and processed unclassified DoD data but were not directly connected to the Global Information Grid. Instead, BlackBerry password requirements were derived using a 2001 protection profile that specified a maximum probability of guessing a system Personal Identification Number for a given Personal Identification Number length and number of access attempts. The Principal Director stated that these policy positions would be clarified in upcoming revisions to DoD Directive 8500.01E and DoD Instruction 8500.2.

Our Response

The Principal Director comments are not responsive. A DoD BlackBerry device that stores and processes DoD information and receives wireless communications that are encrypted at a BES meets the DoD Instruction 8500.2 definition of an information system.[8] In addition, a DoD BlackBerry device can also contain sensitive DoD information, such as personally identifiable information. As a result, we disagree with the Principal Director's position that password requirements for information systems in DoD Instruction 8500.2 do not directly apply to BlackBerry devices. DoD Instruction 8500.2 provides password length and complexity requirements when a user login identifier is used with a password to access a system processing sensitive information. Because just a password could provide access to sensitive information in a BlackBerry device, a DoD BlackBerry device password should, at a minimum, follow the length and complexity requirements of DoD Instruction 8500.2. Furthermore, the Principal Director agreed there should be a uniform length and complexity requirement for passwords for BlackBerry devices throughout the DoD. We request that the Principal Director reconsider his position and provide revised comments in response to the final report.

b. Develop a written plan to implement the use of two-factor authentication for accessing information on BlackBerry devices.

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

The Principal Director partially agreed, stating that while two-factor authentication is desirable for BlackBerry devices, there are currently no suitable second factor products available and none are on the horizon. The Principal Director further stated he would develop an appropriate course of action when such products become available.

Our Response

The comments from the Principal Director are not responsive. We disagree that no action should be taken until a suitable second factor product becomes available. DoD Security Technical Implementation Guide, "Access Control in Support of Information Systems," Version 2, Release 2, December 26, 2008, requires two-factor authentication to access information systems processing sensitive information. In addition, DoD

[8] DoD Instruction 8500.2 defines an information system as a set of information resources organized for collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. DoD requires that a BES be used with BlackBerry devices, which constitutes a set of information resources.

Directive 8521.01E, “Department of Defense Biometrics,” February 21, 2008, states that the ASD(NII)/DoD CIO must ensure that biometrics are developed for access control and effectively integrated into information assurance efforts. Although DoD BlackBerry devices can contain sensitive information, the Principal Director comments provide no information on DoD efforts to ensure that technologies, such as biometrics, are developed and effectively integrated to implement two-factor authentication for BlackBerry devices. A documented plan with milestones would provide a mechanism for DoD to establish a goal, focus DoD efforts, and measure progress on achieving two-factor authentication to protect sensitive information on DoD BlackBerry devices. We request that the Principal Director reconsider his position and provide revised comments in response to the final report.

c. Ensure that the correct risk levels are assigned to all BlackBerry security controls and ensure that only high and medium risk levels are designated as “required.”

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

The Principal Director partially agreed, stating that he will coordinate with DISA to ensure that the correct risk levels are assigned to BlackBerry controls. However, the Principal Director stated that the fact that a security setting is “required” in a Security Technical Implementation Guide does not automatically mean it should be high or medium risk. The issue is the consequence of not applying the settings relative to impact. The consequences of not applying a setting for a low impact control are obviously less than those for a high impact control. The Principal Director further stated that security settings that are required should be applied unless there are compelling operational reasons for not applying the settings. In such a case, the risk should be accepted by the Designated Approving Authority and the rationale explained in a Plan of Action and Milestones.

Our Response

The Principal Director comments are partially responsive. We agree that the Principal Director should coordinate with DISA to ensure the correct risk levels are assigned to BlackBerry controls and that risk levels should be assigned based on the consequence of not applying the control. Although the September 2008 DoD BlackBerry Security Checklist indicates that required controls are mandatory, DoD Instruction 8510.01 gives the Designated Approving Authority the option to accept the risk and authorize a system to operate without correcting low risk weaknesses. Therefore, low risk controls should not be designated as required in the DoD BlackBerry Security Checklist. We request that the Principal Director reconsider his position and provide revised comments in response to the final report. The revised comments should also include an estimated date for completion of management actions.

d. Assign a higher risk level to the data-at-rest encryption and user agreement controls.

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

The Principal Director partially agreed, stating that the DoD Information Assurance Certification and Accreditation Process Technical Advisory Group is currently reviewing and updating Severity Category definitions. The data-at-rest encryption vulnerability and user agreement vulnerability will be reviewed and categorized appropriately when the new definitions are published.

Our Response

The Principal Director comments are partially responsive. We agree that Severity Categories should be reviewed and updated; however, DoD should carefully consider the risk level assigned to the data-at-rest encryption and user agreement controls. For example, data-at-rest encryption is assigned a low level of risk in the September 2008 DoD BlackBerry Security Checklist even though this control could prevent unauthorized access to information, which is more consistent with a higher level of risk. In addition, user agreement is assigned a low level of risk in the September 2008 DoD BlackBerry Security Checklist; however, the November 2007 BlackBerry Security Checklist assigned a medium level of risk to the user agreement. Furthermore, ASD(NII)/DoD CIO representatives stated that the user agreement control should not be assigned a low level of risk. We agree that DoD should not assign a low level of risk to user agreements. Furthermore, DoD should also not assign a low level of risk to data-at-rest encryption. We request that the Principal Director provide revised comments on Recommendation 1.d in response to the final report. The revised comments should include an estimated date for completion of management actions.

e. Require that the seven topics listed in the April 2009 DoD BlackBerry Security Checklist be included in user agreements.

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

The Principal Director agreed, stating that this recommendation was implemented by DISA in the June 26, 2009, release of the Wireless Security Technical Implementation Guide BlackBerry Security Checklist (V5R3) (June 2009 DoD BlackBerry Security Checklist).

Our Response

The comments from the Principal Director are only partially responsive because the June 2009 DoD BlackBerry Security Checklist does not clearly require that all seven topics be included.

Specifically, for three of the seven topics, the June 2009 DoD BlackBerry Security Checklist states that:

- the agreement should contain the type of access required by the user;
- the agreement should contain the responsibilities, liabilities, and security measures; and
- the policy should contain general security requirements and practices.

The November 2007 DoD Wireless Security Technical Implementation Guide states that the word "should" is a recommendation while the word "will" indicates mandatory compliance. In addition, the November 2007 and September 2008 DoD BlackBerry Security Checklists use the word "will" for the three topics above. We request that the Principal Director reconsider his position and provide revised comments in response to the final report. The revised comments should include an estimated date for completion of management actions.

f. Clarify the specific wireless topics required by DoD Directive 8100.02 and establish controls to help ensure users of DoD wireless devices receive annual information assurance training that includes wireless topics.

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

The Principal Director disagreed, stating that mandating specific training in a DoD policy limits the flexibility of the policy and types of training that can be provided for users and administrators. The Principal Director further stated that using the Security Technical Implementation Guides and associated checklists, which are more frequently updated to identify specific wireless training requirements from year-to-year and ensuring those topics are covered, is more beneficial to the security posture than a DoD policy. The Principal Director also stated that the September 2008 release of the Wireless Security Technical Implementation Guide BlackBerry Security Checklist (V5R2.2) consolidated user training requirements into a single vulnerability.

Our Response

The comments from the Principal Director are partially responsive. We agree that the Security Technical Implementation Guides and associated checklists could be used to identify wireless topics for annual training. However, the September 2008 DoD BlackBerry Security Checklist only includes a control to train BlackBerry users on specific topics before the user is issued a BlackBerry device, but the control does not require that those topics also be used in annual information assurance training. In addition, the Principal Director's comments did not specify what controls would be established to help ensure that users of wireless devices receive annual information assurance training that includes wireless topics. We request that the Principal Director reconsider his position and provide revised comments in response to the final report. The revised comments should also include an estimated date for completion of management actions.

2. We recommend that the Air Force Chief Information Officer:

a. Reconcile the various Personal Digital Assistant password requirements in Air Force Instruction 33-200 to determine specific password requirements that Personal Digital Assistant users must follow and adjust Air Force Instruction 33-200 accordingly.

b. Implement controls to ensure that all transactions that affect the inventory of BlackBerry devices are recorded in their Asset Inventory Management System and use the system to accurately respond to official data calls, such as the encryption data call from the Assistant Secretary of Defense (Networks and Information Integration) DoD Chief Information Officer in 2008.

c. Ensure that all security settings are validated and a written authority to operate is issued covering the BlackBerry Enterprise Server that services Andrews and Bolling Air Force Bases.

Management Comments Required

We did not receive comments from the Air Force CIO prior to issuance of the final report. We request that the ASD(NII)/DoD CIO provide revised comments on the final report by October 25, 2009 and that the Air Force CIO also provide comments by October 25, 2009.

Appendix A. Scope and Methodology

We conducted this performance audit from February 2008 through July 2009 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 finding and conclusion based on our audit objectives.

As discussed in the Background, DoD Components reported approximately 63,000 BlackBerry devices used within DoD that have the ability to process sensitive information. We focused the audit on the Air Force, DCMA, DISA and DLA because they accounted for over 55 percent (34,961) of the BlackBerry devices reported to DoD. We visited various Air Force, DCMA, DISA and DLA locations to assess their controls over BlackBerry devices. Specifically, we assessed:

- inventory records to assess their accuracy;
- system security authorization agreements to determine whether the Designated Approving Authority approved the BlackBerry system for use;
- DoD Component user agreements to determine whether the agreement contained the subjects required by the DoD BlackBerry Security Checklist;
- each DoD Component’s annual information assurance training courses to determine whether it contained wireless topics, as required by DoD Directive 8100.02;
- BES policy settings at each DoD Component to determine whether the password settings were in compliance with the DoD BlackBerry Security Checklist and to determine whether each DoD Component had implemented data-at-rest encryption, as required by the JTF-GNO CTO 08-009; and
- the physical security of each DoD Component’s BES to ensure the server was protected from unauthorized access.

We reviewed the following primary criteria governing BlackBerry devices:

- DoD Directive 8100.02, “ Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid,” April 14, 2004;
- DoD Wireless Security Technical Implementation Guide, Version 5, Release 2, November 15, 2007;
- DoD Wireless Security Technical Implementation Guide, BlackBerry Security Checklist, Version 5, Release 2.1, November 15, 2007;
- DoD Wireless Security Technical Implementation Guide, BlackBerry Security Checklist, Version 5, Release 2.2, September 15, 2008; and
- Joint Task Force Global Network Operations Communications Tasking Orders.

We obtained assistance from the Quantitative Methods and Analysis Division in selecting a sample of users to review at specific Air Force, DCMA, DISA, and DLA locations.

Specifically, the Quantitative Methods and Analysis Division selected a stratified sample of 971 devices out of a universe of 4,374 BlackBerry devices to determine whether the Air Force, DCMA, DISA, and DLA Blackberry devices were configured in accordance with the BES settings for password character length and inventory controls. Due to the inability to test the entire sample because of the transient nature of the BlackBerry users and identification of clearer ways to present the information we did not use the results from the sample.

Use of Computer-Processed Data

We used computer processed data to determine which DoD Components we would visit to test controls over information contained in BlackBerry devices. The DoD Components reported to ASD(NII)/DoD CIO that, as of January 2008, DoD used approximately 63,000 BlackBerry devices that contained sensitive information. We used this universe to determine the DoD Components that used the greatest number of BlackBerry devices. After reviewing Air Force inventory records, we cannot be certain that the Air Force reported an accurate number of BlackBerry devices with encryption to ASD(NII)/DoD CIO, which affected the overall accuracy of BlackBerry devices reported to ASD(NII)/DoD CIO. We did not have the resources to review the accuracy of inventory records reported by all DoD Components that made up the entire database of 63,000 devices. Although the total number of BlackBerry devices reported to ASD(NII)/DoD CIO may not be accurate, it did not affect the overall results and conclusions made in this report. Specifically, we limited the use of information reported to ASD(NII)/DoD CIO to Background and scope information.

Prior Coverage

During the last five years, the Government Accountability Office (GAO) and the DoD Inspector General (DoD IG) have issued six reports discussing the security controls over wireless devices. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-08-525, “Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains,” June 27, 2008

GAO Report No. GAO-08-343, “Protecting Personally Identifiable Information,” January 25, 2008

GAO Report No. GAO-07-935T, “Agencies Report Progress, but Sensitive Data Remain at Risk,” June 7, 2007

GAO Report No. GAO-06-833T, “Preventing and Responding to Improper Disclosures of Personal Information,” June 8, 2006

GAO Report No. GAO-05-383, “Federal Agencies Need to Improve Controls over Wireless Networks,” May 17, 2005

DoD IG

DoD IG Report No. D-2006-052, “DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements,” February 23, 2006

Appendix B. Defense Contract Management Agency Comments

The DCMA Executive Director for Information Technology and CIO (DCMA CIO) commented on the Finding and recommendations. Based on DCMA CIO comments, we revised the finding discussion to state that DCMA excluded the BlackBerry address book from content protection. For the full text of DCMA CIO comments, see the Management Comments section of the report.

DCMA Comments on Password Compliance

DCMA CIO agreed that DCMA did not always meet the password length and complexity requirements of DoD Instruction 8500.2 to protect sensitive information. However, the DCMA CIO noted that the DCMA was in compliance with the DoD BlackBerry Security Checklist password complexity and length requirements.

Our Response

DCMA met password length and complexity requirements in accordance with the DoD BlackBerry Security Checklist. However, because BlackBerry devices can contain sensitive DoD information, we recommend that ASD(NII)/DoD CIO revise the DoD BlackBerry Security Checklist to require passwords for BlackBerry devices to be in accordance with the DoD Instruction 8500.2 for protecting sensitive information.

DCMA Comments on Implementing Discretionary Controls

DCMA CIO agreed that the DCMA Designated Approving Authority did not always implement “required” controls that were assigned a low risk. The DCMA CIO noted that DCMA used their discretion in not implementing some controls assigned a low level of risk as permitted by DoD Instruction 8510.01.

Our Response

DoD Instruction 8510.01 allowed DCMA to use their discretion in not implementing “required” controls assigned a low level of risk. As a result, we recommend that DoD ensure that the correct risk levels are assigned to all BlackBerry security controls and ensure that only high and medium risk levels are designated as “required.”

DCMA Comments on Encryption of Data Stored on BlackBerry Devices

DCMA CIO partially agreed that DCMA did not always encrypt data stored on BlackBerry devices. Specifically, the DCMA CIO noted that during the audit, DCMA encrypted all data on their BlackBerry devices except the address book. The DCMA CIO stated that the control was assigned a low risk, which allowed them to use their discretion in not implementing the control.

Our Response

The control to encrypt data stored on BlackBerry devices was assigned a low risk, which allowed DCMA personnel to use their discretion in implementing the control. As the report states, DCMA encrypted the data stored on their BlackBerry devices, excluding the address book. Therefore, because encrypting data stored on BlackBerry devices can prevent unauthorized access to information, we recommend that DoD assign a higher risk level to the data-at-rest encryption control.

DCMA Comments on BlackBerry User Agreements

DCMA CIO partially agreed that DCMA did not properly educate BlackBerry users on their roles and responsibilities when using the BlackBerry device. Specifically, DCMA CIO stated that the DCMA Computer Security Awareness Training (annual information assurance training) included the required seven user agreement topics and was substituted for the BlackBerry user agreement. DCMA CIO further stated that the DCMA annual information assurance training has included the seven user agreement topics since 2004.

Our Response

In July 2008, DCMA management was informed that their FY 2008 annual information assurance training did not include the seven user agreement topics. DCMA management stated that they were not aware of the BlackBerry user agreement requirement. Subsequently, DCMA management developed additional annual information assurance training material, which included six of seven user agreement topics.

DCMA Comments on Password Expiration and Device Lock out

DCMA CIO agreed that DCMA did not always configure their BES to require BlackBerry device passwords to expire and lock out after a specified period of time. DCMA CIO noted that the September 2008 DoD BlackBerry Security Checklist assigned a low level of risk to these requirements. DCMA CIO stated that during the course of the audit, DCMA implemented the password lockout requirement.

Our Response

The password expiration and device lockout controls were assigned a low risk, which allowed DCMA to use their discretion in implementing the control. However, as the report states, DCMA took steps to implement the BES configurations for password requirements.

DCMA Comments on Annual Information Assurance Training

DCMA CIO disagreed with the statement that the DCMA annual information assurance training did not always include wireless topics. Specifically, the CIO noted that although the DCMA annual information assurance training did not specifically address BlackBerry devices, the training has always included wireless topics.

Our Response

In July 2008, DCMA management was informed that their FY 2008 annual information assurance training did not include wireless topics. Subsequently, DCMA management implemented additional annual information assurance training material, which included wireless topics.

DCMA Comments on Encrypting the BlackBerry Address Book

DCMA CIO partially agreed with the statement that DCMA permitted its users to not encrypt their address book. Specifically, the CIO noted that DCMA did not encrypt the address book.

Our Response

Based on DCMA CIO comments, we revised the Finding discussion to state, "DCMA excluded the address book from content protection."

Defense Contract Management Agency Comments on the Recommendation

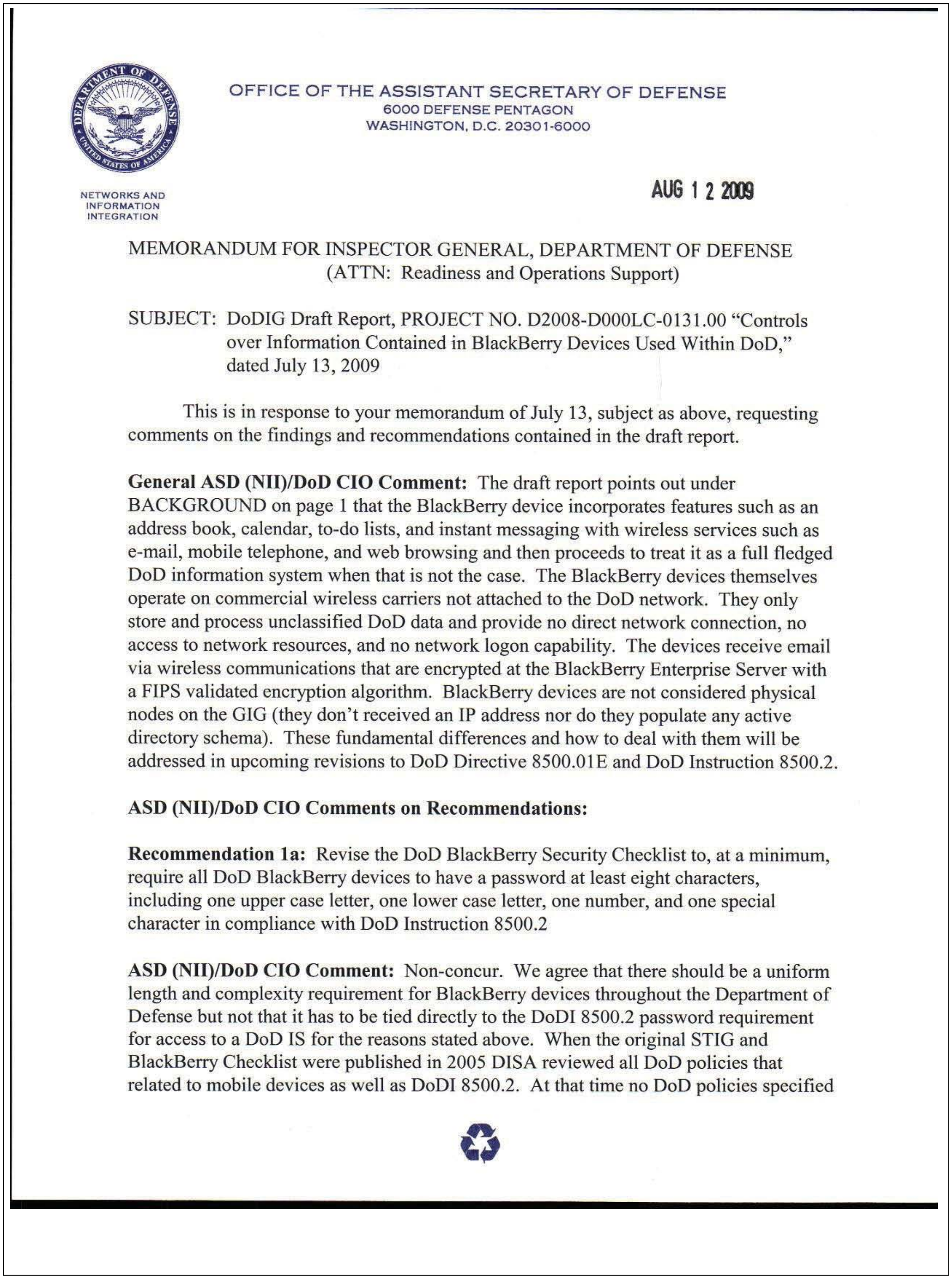
DCMA CIO agreed with Recommendations 1.a-c and 1.f. DCMA CIO partially agreed with Recommendation 1.d., stating that the user agreement should be assigned a low level of risk and periodic training is more effective than one-time user agreements. However, the DCMA CIO did not agree with Recommendation 1.e., stating that the implementation of Recommendation 1.f would be sufficient.

Our Response

User agreements are particularly important for mobile and remote users because there is a high risk of lost, theft, or compromise. A signed user agreement helps to ensure that users are made aware of risks and proper procedures for BlackBerry devices. In addition, the November 2007 BlackBerry Security Checklist assigned a higher level of risk to user agreements, and ASD(NII)/DoD CIO representatives stated that user agreements should not be assigned a low level of risk.

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

Final Report
Reference



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

NETWORKS AND
INFORMATION
INTEGRATION

AUG 12 2009

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: Readiness and Operations Support)

SUBJECT: DoDIG Draft Report, PROJECT NO. D2008-D000LC-0131.00 "Controls over Information Contained in BlackBerry Devices Used Within DoD," dated July 13, 2009

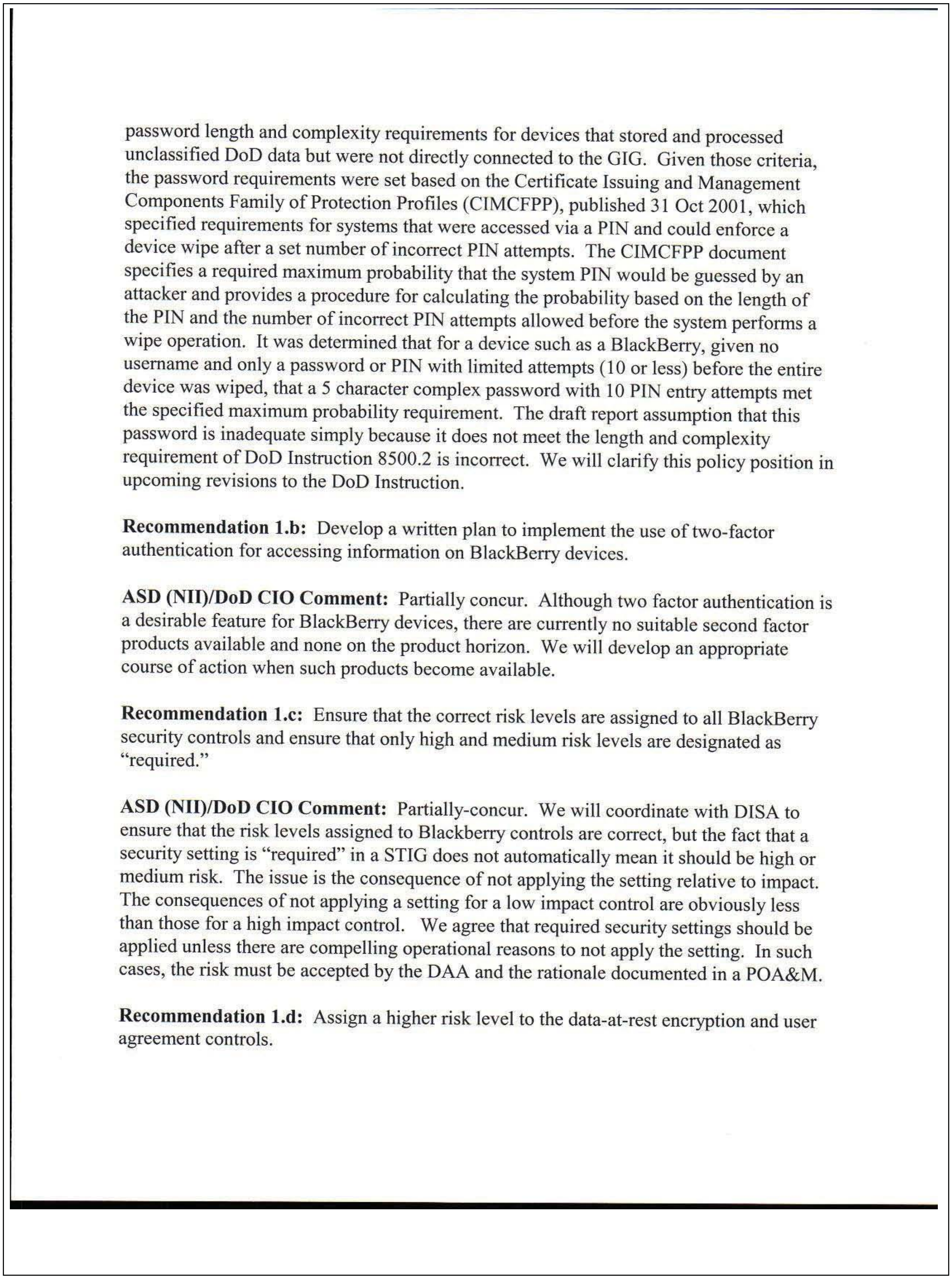
This is in response to your memorandum of July 13, subject as above, requesting comments on the findings and recommendations contained in the draft report.

General ASD (NII)/DoD CIO Comment: The draft report points out under BACKGROUND on page 1 that the BlackBerry device incorporates features such as an address book, calendar, to-do lists, and instant messaging with wireless services such as e-mail, mobile telephone, and web browsing and then proceeds to treat it as a full fledged DoD information system when that is not the case. The BlackBerry devices themselves operate on commercial wireless carriers not attached to the DoD network. They only store and process unclassified DoD data and provide no direct network connection, no access to network resources, and no network logon capability. The devices receive email via wireless communications that are encrypted at the BlackBerry Enterprise Server with a FIPS validated encryption algorithm. BlackBerry devices are not considered physical nodes on the GIG (they don't received an IP address nor do they populate any active directory schema). These fundamental differences and how to deal with them will be addressed in upcoming revisions to DoD Directive 8500.01E and DoD Instruction 8500.2.

ASD (NII)/DoD CIO Comments on Recommendations:

Recommendation 1a: Revise the DoD BlackBerry Security Checklist to, at a minimum, require all DoD BlackBerry devices to have a password at least eight characters, including one upper case letter, one lower case letter, one number, and one special character in compliance with DoD Instruction 8500.2

ASD (NII)/DoD CIO Comment: Non-concur. We agree that there should be a uniform length and complexity requirement for BlackBerry devices throughout the Department of Defense but not that it has to be tied directly to the DoDI 8500.2 password requirement for access to a DoD IS for the reasons stated above. When the original STIG and BlackBerry Checklist were published in 2005 DISA reviewed all DoD policies that related to mobile devices as well as DoDI 8500.2. At that time no DoD policies specified



password length and complexity requirements for devices that stored and processed unclassified DoD data but were not directly connected to the GIG. Given those criteria, the password requirements were set based on the Certificate Issuing and Management Components Family of Protection Profiles (CIMCFPP), published 31 Oct 2001, which specified requirements for systems that were accessed via a PIN and could enforce a device wipe after a set number of incorrect PIN attempts. The CIMCFPP document specifies a required maximum probability that the system PIN would be guessed by an attacker and provides a procedure for calculating the probability based on the length of the PIN and the number of incorrect PIN attempts allowed before the system performs a wipe operation. It was determined that for a device such as a BlackBerry, given no username and only a password or PIN with limited attempts (10 or less) before the entire device was wiped, that a 5 character complex password with 10 PIN entry attempts met the specified maximum probability requirement. The draft report assumption that this password is inadequate simply because it does not meet the length and complexity requirement of DoD Instruction 8500.2 is incorrect. We will clarify this policy position in upcoming revisions to the DoD Instruction.

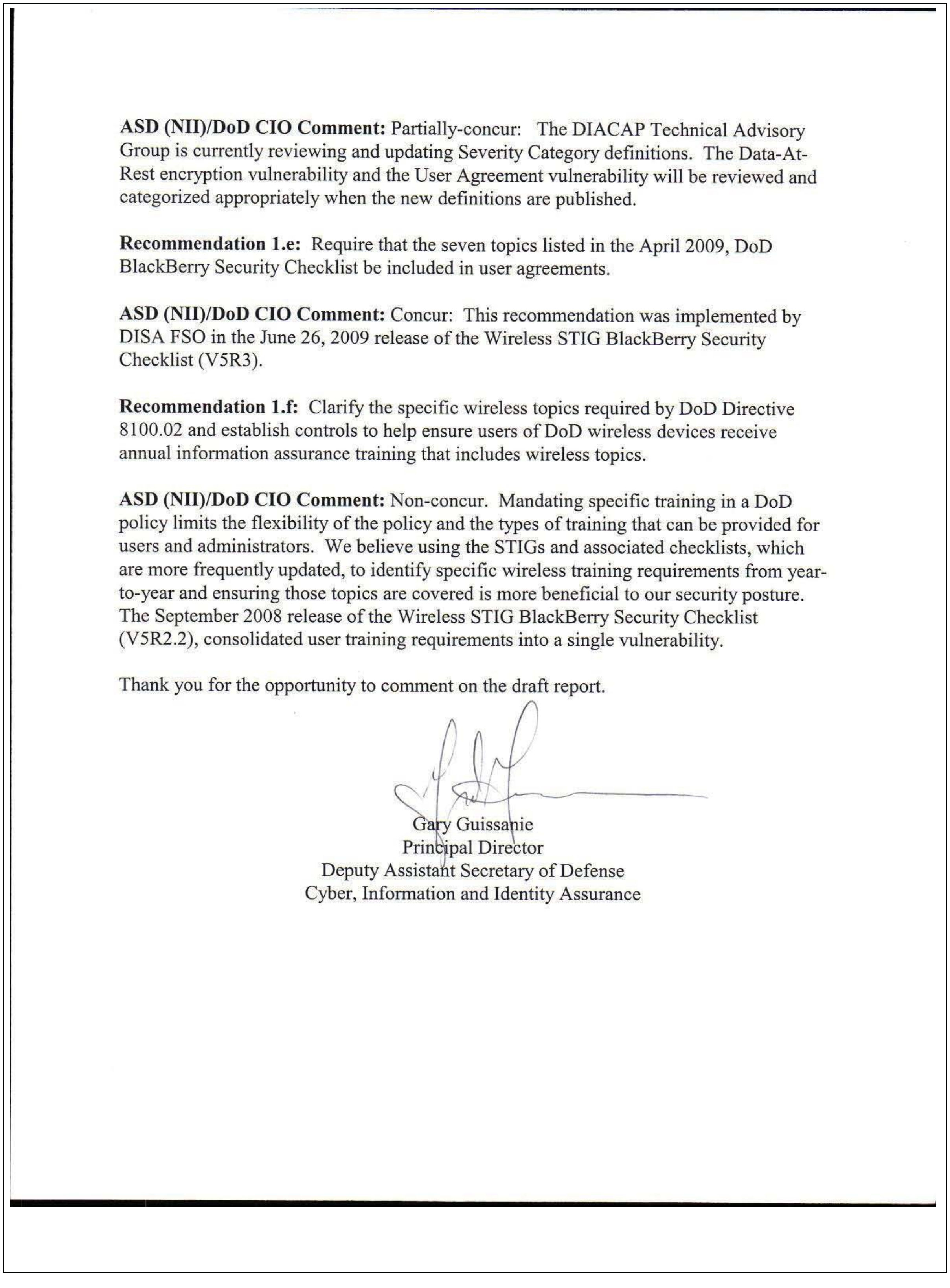
Recommendation 1.b: Develop a written plan to implement the use of two-factor authentication for accessing information on BlackBerry devices.

ASD (NII)/DoD CIO Comment: Partially concur. Although two factor authentication is a desirable feature for BlackBerry devices, there are currently no suitable second factor products available and none on the product horizon. We will develop an appropriate course of action when such products become available.

Recommendation 1.c: Ensure that the correct risk levels are assigned to all BlackBerry security controls and ensure that only high and medium risk levels are designated as "required."

ASD (NII)/DoD CIO Comment: Partially-concur. We will coordinate with DISA to ensure that the risk levels assigned to Blackberry controls are correct, but the fact that a security setting is "required" in a STIG does not automatically mean it should be high or medium risk. The issue is the consequence of not applying the setting relative to impact. The consequences of not applying a setting for a low impact control are obviously less than those for a high impact control. We agree that required security settings should be applied unless there are compelling operational reasons to not apply the setting. In such cases, the risk must be accepted by the DAA and the rationale documented in a POA&M.

Recommendation 1.d: Assign a higher risk level to the data-at-rest encryption and user agreement controls.



ASD (NII)/DoD CIO Comment: Partially-concur: The DIACAP Technical Advisory Group is currently reviewing and updating Severity Category definitions. The Data-At-Rest encryption vulnerability and the User Agreement vulnerability will be reviewed and categorized appropriately when the new definitions are published.

Recommendation 1.e: Require that the seven topics listed in the April 2009, DoD BlackBerry Security Checklist be included in user agreements.

ASD (NII)/DoD CIO Comment: Concur: This recommendation was implemented by DISA FSO in the June 26, 2009 release of the Wireless STIG BlackBerry Security Checklist (V5R3).

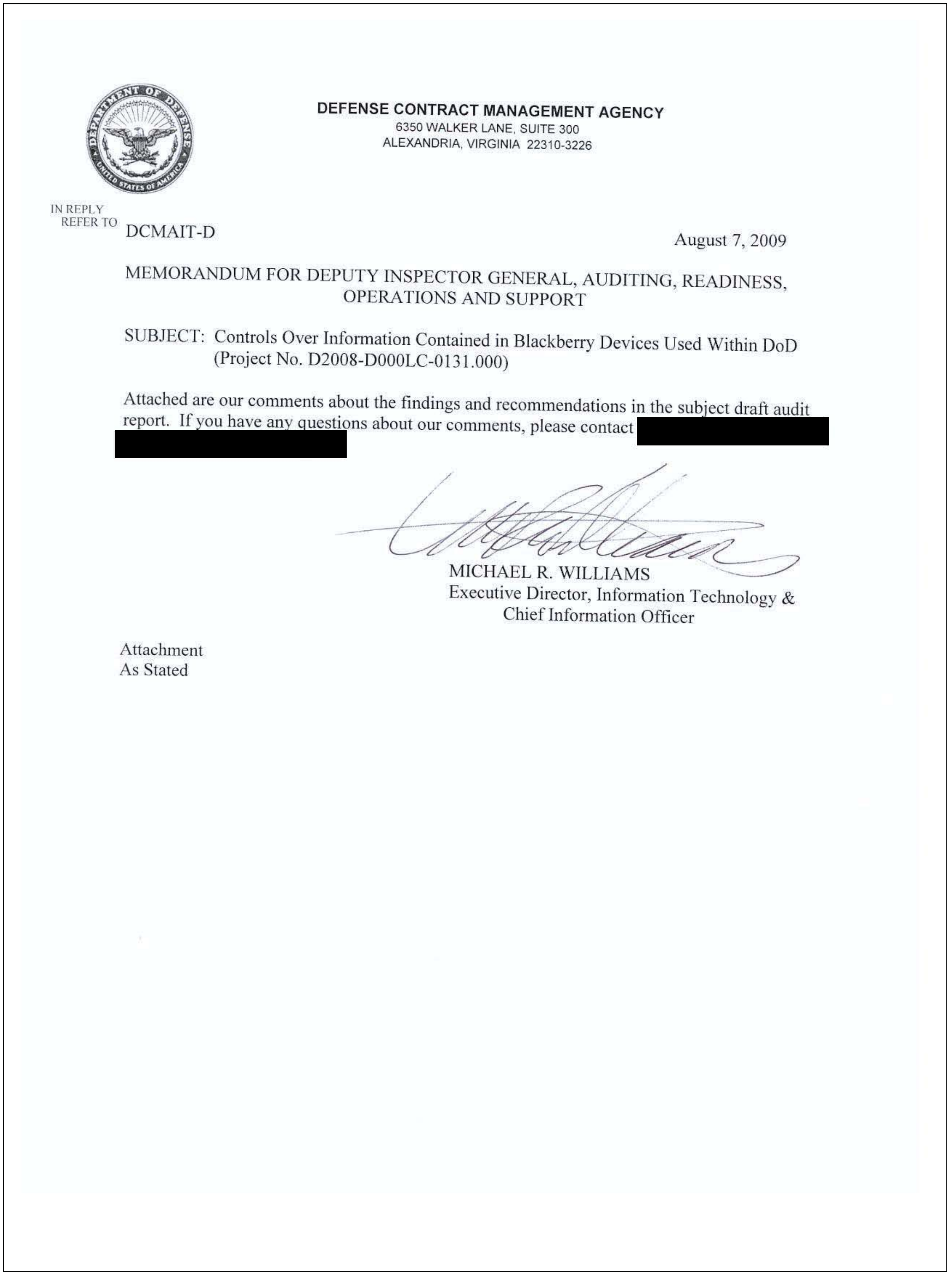
Recommendation 1.f: Clarify the specific wireless topics required by DoD Directive 8100.02 and establish controls to help ensure users of DoD wireless devices receive annual information assurance training that includes wireless topics.

ASD (NII)/DoD CIO Comment: Non-concur. Mandating specific training in a DoD policy limits the flexibility of the policy and the types of training that can be provided for users and administrators. We believe using the STIGs and associated checklists, which are more frequently updated, to identify specific wireless training requirements from year-to-year and ensuring those topics are covered is more beneficial to our security posture. The September 2008 release of the Wireless STIG BlackBerry Security Checklist (V5R2.2), consolidated user training requirements into a single vulnerability.

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

Gary Guissanie
Principal Director
Deputy Assistant Secretary of Defense
Cyber, Information and Identity Assurance

Defense Contract Management Agency Comments



DEFENSE CONTRACT MANAGEMENT AGENCY
6350 WALKER LANE, SUITE 300
ALEXANDRIA, VIRGINIA 22310-3226

IN REPLY
REFER TO DCMAIT-D

August 7, 2009

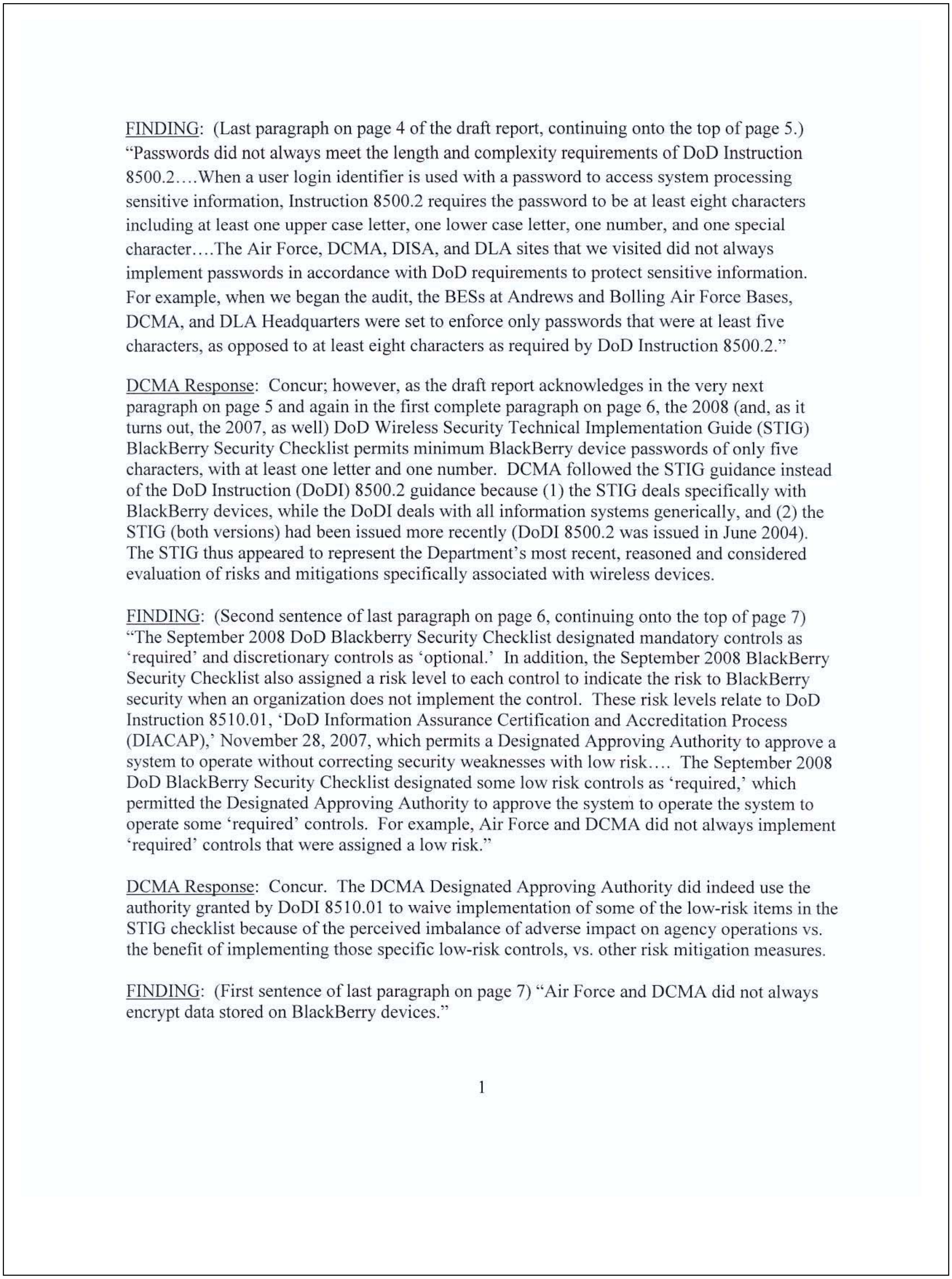
MEMORANDUM FOR DEPUTY INSPECTOR GENERAL, AUDITING, READINESS, OPERATIONS AND SUPPORT

SUBJECT: Controls Over Information Contained in Blackberry Devices Used Within DoD (Project No. D2008-D000LC-0131.000)

Attached are our comments about the findings and recommendations in the subject draft audit report. If you have any questions about our comments, please contact [redacted]

MICHAEL R. WILLIAMS
Executive Director, Information Technology &
Chief Information Officer

Attachment
As Stated



FINDING: (Last paragraph on page 4 of the draft report, continuing onto the top of page 5.) "Passwords did not always meet the length and complexity requirements of DoD Instruction 8500.2….When a user login identifier is used with a password to access system processing sensitive information, Instruction 8500.2 requires the password to be at least eight characters including at least one upper case letter, one lower case letter, one number, and one special character….The Air Force, DCMA, DISA, and DLA sites that we visited did not always implement passwords in accordance with DoD requirements to protect sensitive information. For example, when we began the audit, the BESs at Andrews and Bolling Air Force Bases, DCMA, and DLA Headquarters were set to enforce only passwords that were at least five characters, as opposed to at least eight characters as required by DoD Instruction 8500.2."

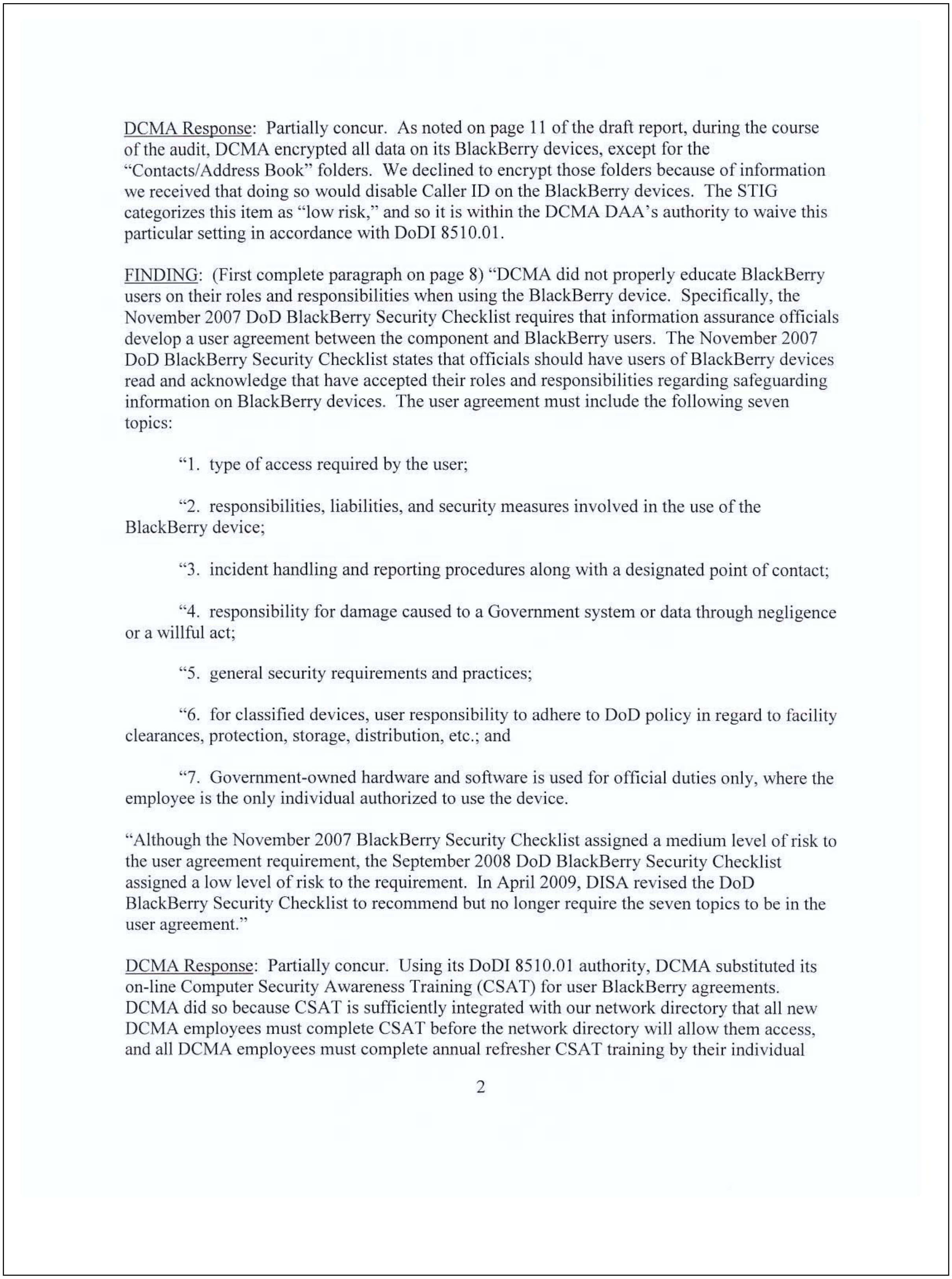
DCMA Response: Concur; however, as the draft report acknowledges in the very next paragraph on page 5 and again in the first complete paragraph on page 6, the 2008 (and, as it turns out, the 2007, as well) DoD Wireless Security Technical Implementation Guide (STIG) BlackBerry Security Checklist permits minimum BlackBerry device passwords of only five characters, with at least one letter and one number. DCMA followed the STIG guidance instead of the DoD Instruction (DoDI) 8500.2 guidance because (1) the STIG deals specifically with BlackBerry devices, while the DoDI deals with all information systems generically, and (2) the STIG (both versions) had been issued more recently (DoDI 8500.2 was issued in June 2004). The STIG thus appeared to represent the Department's most recent, reasoned and considered evaluation of risks and mitigations specifically associated with wireless devices.

Revised page 6

FINDING: (Second sentence of last paragraph on page 6, continuing onto the top of page 7) "The September 2008 DoD Blackberry Security Checklist designated mandatory controls as 'required' and discretionary controls as 'optional.' In addition, the September 2008 BlackBerry Security Checklist also assigned a risk level to each control to indicate the risk to BlackBerry security when an organization does not implement the control. These risk levels relate to DoD Instruction 8510.01, 'DoD Information Assurance Certification and Accreditation Process (DIACAP),' November 28, 2007, which permits a Designated Approving Authority to approve a system to operate without correcting security weaknesses with low risk…. The September 2008 DoD BlackBerry Security Checklist designated some low risk controls as 'required,' which permitted the Designated Approving Authority to approve the system to operate the system to operate some 'required' controls. For example, Air Force and DCMA did not always implement 'required' controls that were assigned a low risk."

DCMA Response: Concur. The DCMA Designated Approving Authority did indeed use the authority granted by DoDI 8510.01 to waive implementation of some of the low-risk items in the STIG checklist because of the perceived imbalance of adverse impact on agency operations vs. the benefit of implementing those specific low-risk controls, vs. other risk mitigation measures.

FINDING: (First sentence of last paragraph on page 7) "Air Force and DCMA did not always encrypt data stored on BlackBerry devices."



DCMA Response: Partially concur. As noted on page 11 of the draft report, during the course of the audit, DCMA encrypted all data on its BlackBerry devices, except for the "Contacts/Address Book" folders. We declined to encrypt those folders because of information we received that doing so would disable Caller ID on the BlackBerry devices. The STIG categorizes this item as "low risk," and so it is within the DCMA DAA's authority to waive this particular setting in accordance with DoDI 8510.01.

FINDING: (First complete paragraph on page 8) "DCMA did not properly educate BlackBerry users on their roles and responsibilities when using the BlackBerry device. Specifically, the November 2007 DoD BlackBerry Security Checklist requires that information assurance officials develop a user agreement between the component and BlackBerry users. The November 2007 DoD BlackBerry Security Checklist states that officials should have users of BlackBerry devices read and acknowledge that have accepted their roles and responsibilities regarding safeguarding information on BlackBerry devices. The user agreement must include the following seven topics:

"1. type of access required by the user;

"2. responsibilities, liabilities, and security measures involved in the use of the BlackBerry device;

"3. incident handling and reporting procedures along with a designated point of contact;

"4. responsibility for damage caused to a Government system or data through negligence or a willful act;

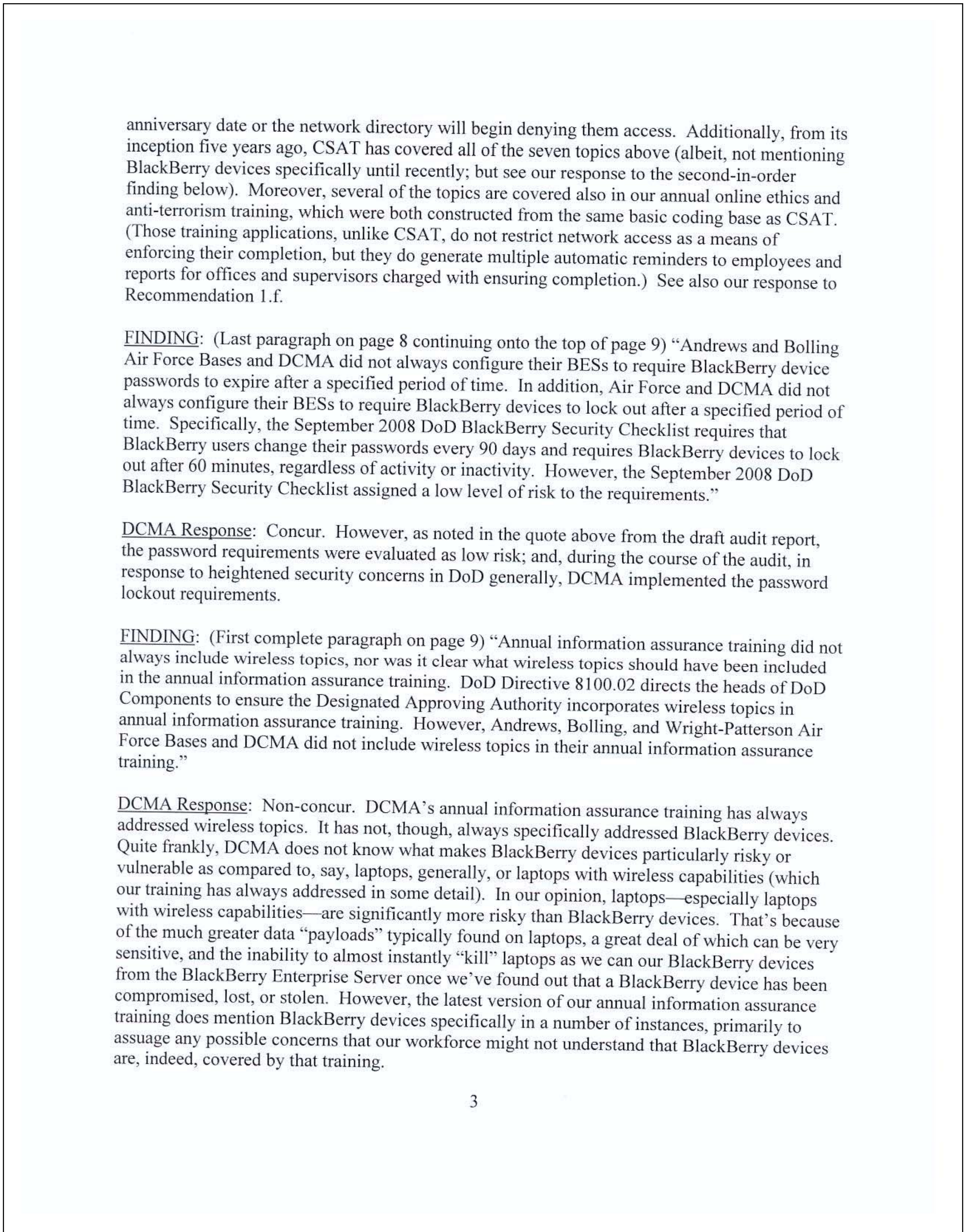
"5. general security requirements and practices;

"6. for classified devices, user responsibility to adhere to DoD policy in regard to facility clearances, protection, storage, distribution, etc.; and

"7. Government-owned hardware and software is used for official duties only, where the employee is the only individual authorized to use the device.

"Although the November 2007 BlackBerry Security Checklist assigned a medium level of risk to the user agreement requirement, the September 2008 DoD BlackBerry Security Checklist assigned a low level of risk to the requirement. In April 2009, DISA revised the DoD BlackBerry Security Checklist to recommend but no longer require the seven topics to be in the user agreement."

DCMA Response: Partially concur. Using its DoDI 8510.01 authority, DCMA substituted its on-line Computer Security Awareness Training (CSAT) for user BlackBerry agreements. DCMA did so because CSAT is sufficiently integrated with our network directory that all new DCMA employees must complete CSAT before the network directory will allow them access, and all DCMA employees must complete annual refresher CSAT training by their individual



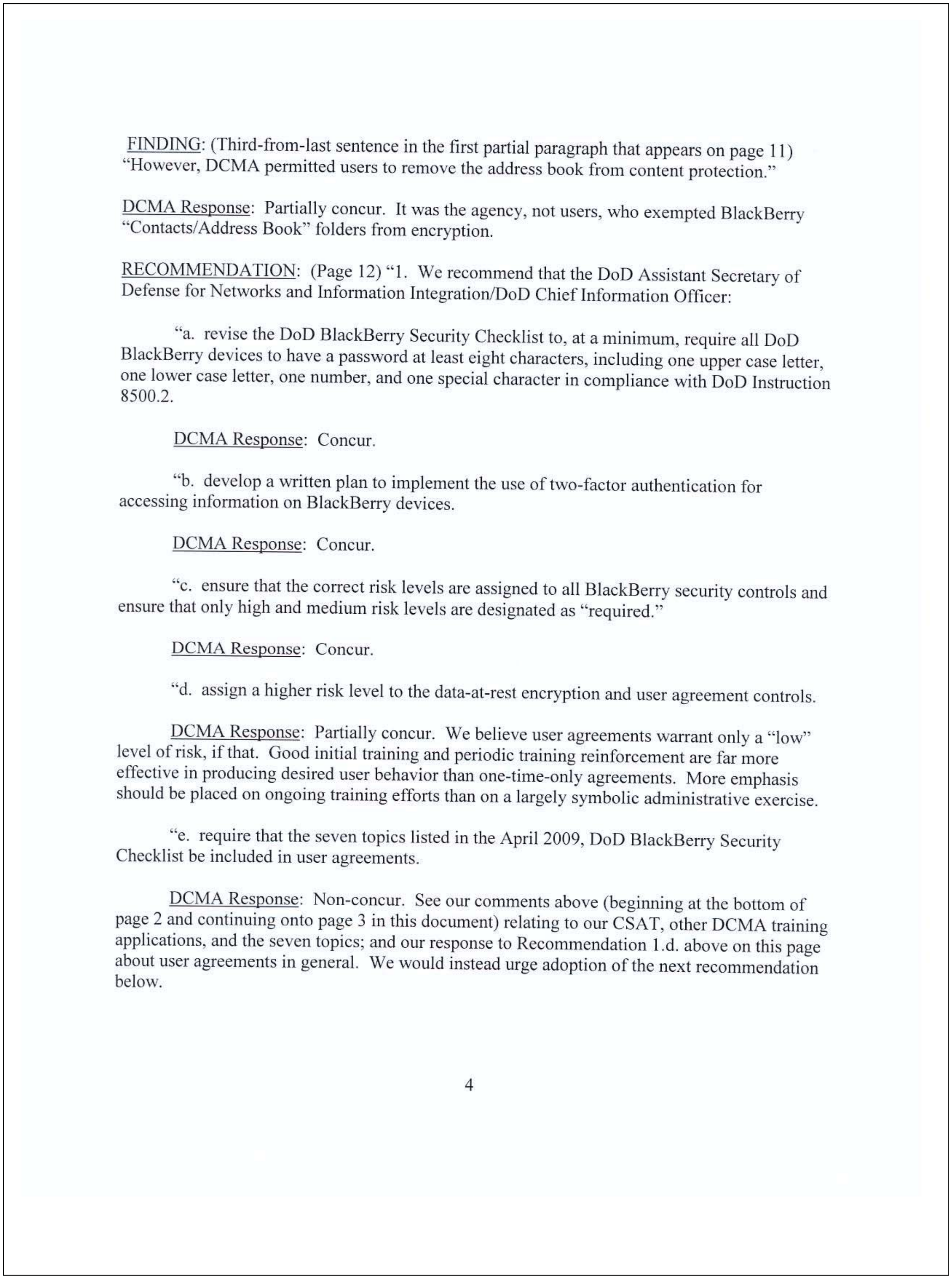
anniversary date or the network directory will begin denying them access. Additionally, from its inception five years ago, CSAT has covered all of the seven topics above (albeit, not mentioning BlackBerry devices specifically until recently; but see our response to the second-in-order finding below). Moreover, several of the topics are covered also in our annual online ethics and anti-terrorism training, which were both constructed from the same basic coding base as CSAT. (Those training applications, unlike CSAT, do not restrict network access as a means of enforcing their completion, but they do generate multiple automatic reminders to employees and reports for offices and supervisors charged with ensuring completion.) See also our response to Recommendation 1.f.

FINDING: (Last paragraph on page 8 continuing onto the top of page 9) "Andrews and Bolling Air Force Bases and DCMA did not always configure their BESs to require BlackBerry device passwords to expire after a specified period of time. In addition, Air Force and DCMA did not always configure their BESs to require BlackBerry devices to lock out after a specified period of time. Specifically, the September 2008 DoD BlackBerry Security Checklist requires that BlackBerry users change their passwords every 90 days and requires BlackBerry devices to lock out after 60 minutes, regardless of activity or inactivity. However, the September 2008 DoD BlackBerry Security Checklist assigned a low level of risk to the requirements."

DCMA Response: Concur. However, as noted in the quote above from the draft audit report, the password requirements were evaluated as low risk; and, during the course of the audit, in response to heightened security concerns in DoD generally, DCMA implemented the password lockout requirements.

FINDING: (First complete paragraph on page 9) "Annual information assurance training did not always include wireless topics, nor was it clear what wireless topics should have been included in the annual information assurance training. DoD Directive 8100.02 directs the heads of DoD Components to ensure the Designated Approving Authority incorporates wireless topics in annual information assurance training. However, Andrews, Bolling, and Wright-Patterson Air Force Bases and DCMA did not include wireless topics in their annual information assurance training."

DCMA Response: Non-concur. DCMA's annual information assurance training has always addressed wireless topics. It has not, though, always specifically addressed BlackBerry devices. Quite frankly, DCMA does not know what makes BlackBerry devices particularly risky or vulnerable as compared to, say, laptops, generally, or laptops with wireless capabilities (which our training has always addressed in some detail). In our opinion, laptops—especially laptops with wireless capabilities—are significantly more risky than BlackBerry devices. That's because of the much greater data "payloads" typically found on laptops, a great deal of which can be very sensitive, and the inability to almost instantly "kill" laptops as we can our BlackBerry devices from the BlackBerry Enterprise Server once we've found out that a BlackBerry device has been compromised, lost, or stolen. However, the latest version of our annual information assurance training does mention BlackBerry devices specifically in a number of instances, primarily to assuage any possible concerns that our workforce might not understand that BlackBerry devices are, indeed, covered by that training.



FINDING: (Third-from-last sentence in the first partial paragraph that appears on page 11) "However, DCMA permitted users to remove the address book from content protection."

DCMA Response: Partially concur. It was the agency, not users, who exempted BlackBerry "Contacts/Address Book" folders from encryption.

Revised page 11

RECOMMENDATION: (Page 12) "1. We recommend that the DoD Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer:

"a. revise the DoD BlackBerry Security Checklist to, at a minimum, require all DoD BlackBerry devices to have a password at least eight characters, including one upper case letter, one lower case letter, one number, and one special character in compliance with DoD Instruction 8500.2.

DCMA Response: Concur.

"b. develop a written plan to implement the use of two-factor authentication for accessing information on BlackBerry devices.

DCMA Response: Concur.

"c. ensure that the correct risk levels are assigned to all BlackBerry security controls and ensure that only high and medium risk levels are designated as "required."

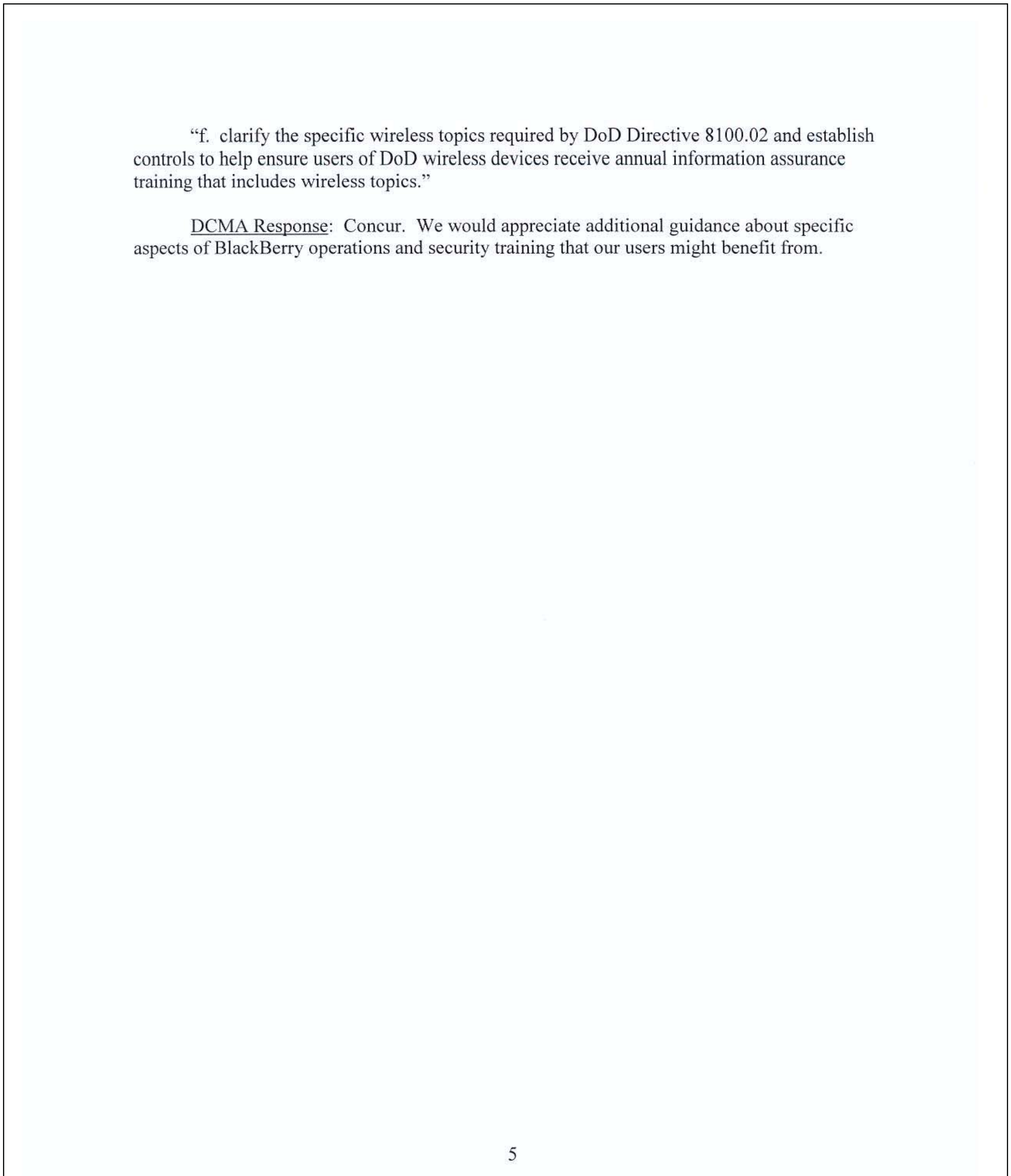
DCMA Response: Concur.

"d. assign a higher risk level to the data-at-rest encryption and user agreement controls.

DCMA Response: Partially concur. We believe user agreements warrant only a "low" level of risk, if that. Good initial training and periodic training reinforcement are far more effective in producing desired user behavior than one-time-only agreements. More emphasis should be placed on ongoing training efforts than on a largely symbolic administrative exercise.

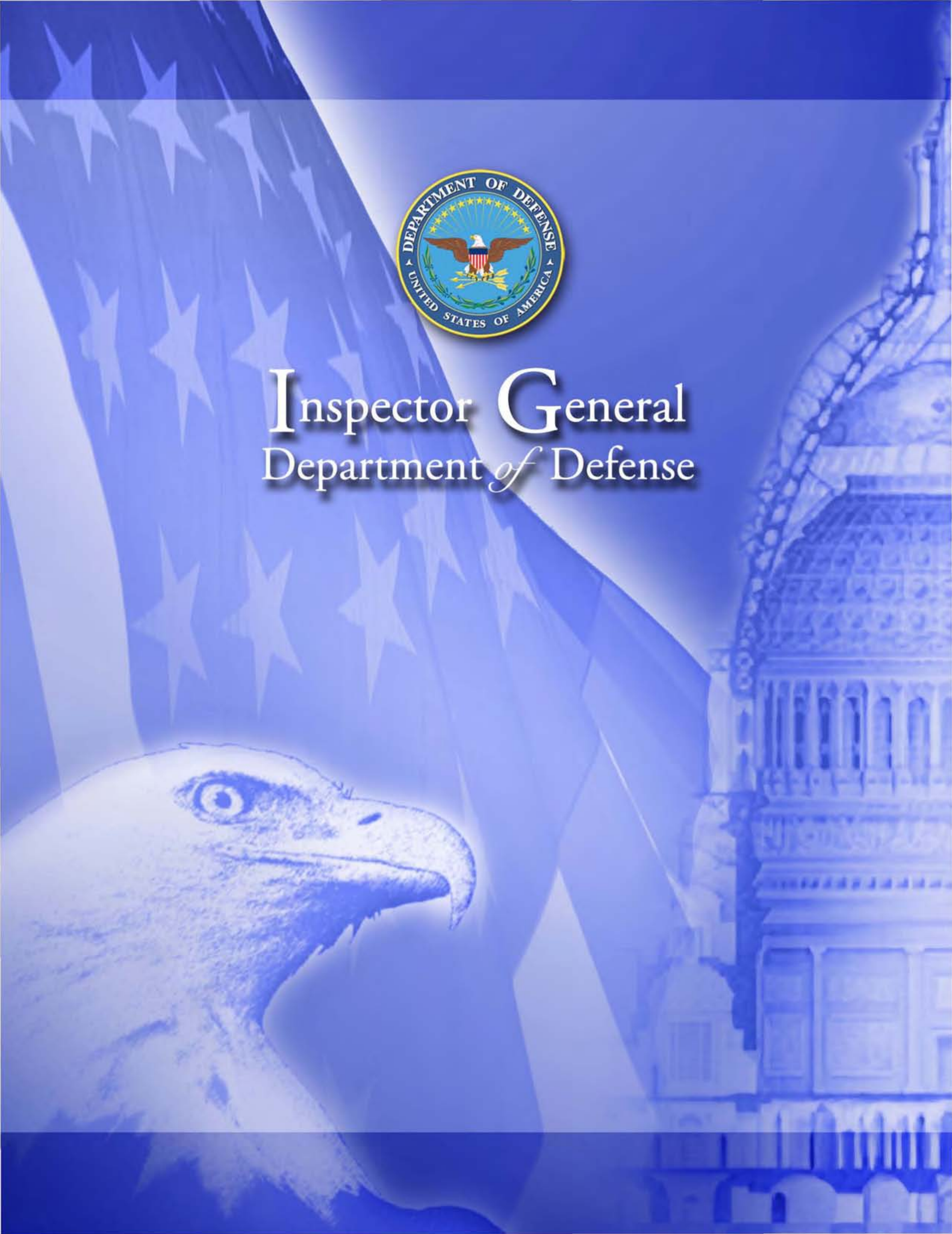
"e. require that the seven topics listed in the April 2009, DoD BlackBerry Security Checklist be included in user agreements.

DCMA Response: Non-concur. See our comments above (beginning at the bottom of page 2 and continuing onto page 3 in this document) relating to our CSAT, other DCMA training applications, and the seven topics; and our response to Recommendation 1.d. above on this page about user agreements in general. We would instead urge adoption of the next recommendation below.



"f. clarify the specific wireless topics required by DoD Directive 8100.02 and establish controls to help ensure users of DoD wireless devices receive annual information assurance training that includes wireless topics."

DCMA Response: Concur. We would appreciate additional guidance about specific aspects of BlackBerry operations and security training that our users might benefit from.



Inspector General
Department of Defense