PROCESSING CLASSIFIED INFORMATION ON PORTABLE COMPUTERS IN THE DEPARTMENT OF JUSTICE

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 05-32
July 2005

PROCESSING CLASSIFIED INFORMATION ON PORTABLE COMPUTERS IN THE DEPARTMENT OF JUSTICE

EXECUTIVE SUMMARY

This Office of the Inspector General audit examines the policies and practices in the Department of Justice (DOJ or Department) regarding classified information on portable computers. Our audit objectives were to: (1) review the Department's policies and practices concerning the storage of classified information on portable computers, and (2) determine whether more effective practices could be adopted by the Department to enhance the ability to process classified information on portable computers while adequately safeguarding the information.

To accomplish our objectives, we interviewed the Department's Deputy Chief Information Officer; the Assistant Director of the Security and Emergency Planning Staff (SEPS); and information technology (IT) security personnel from the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the Executive Office for United States Attorneys (EOUSA). In addition, we interviewed IT security personnel from the Central Intelligence Agency (CIA), the National Security Agency, the National Reconnaissance Office (within the Department of Defense), and the Department of Energy. We also analyzed both government-wide policy and DOJ policy as they relate to the processing of classified information on portable computers.

Government-wide Policy

Three organizations have responsibility for developing government-wide policy related to the certification and accreditation of IT systems.[1] The *Federal Information Security Management Act* (FISMA) delegates policy development and oversight to the National Institute of Standards and Technology (NIST) for information systems other than national security systems. Executive Order 13231, *Critical Infrastructure*

[1] Certification and accreditation is a comprehensive evaluation of the technical and non-technical security features and other safeguards in place on a system. The certification is made as part of and in support of the accreditation process. The certification process validates that appropriate safeguards have been implemented on the system. The process culminates in the accreditation of the system (permission for the system to operate).

Protection, requires the Committee on National Security Systems (CNSS) to develop policy over national security systems that store, process, or transmit classified information.[2] In addition, Executive Orders 12333 and 12958 delegates to the CIA the responsibility for developing policy related to processing Sensitive Compartmented Information.[3] Based on Executive Orders, the CNSS and the CIA are the ultimate authorities on how Classified National Security Information and Sensitive Compartmented Information are to be processed on computers within the DOJ and throughout the federal government. The policies developed by these organizations cover all IT systems, including portable computers.

DOJ Policy

DOJ Order 2640.2E establishes uniform policy, responsibilities, and authorities for the implementation and protection of the DOJ's IT systems that store, process, or transmit classified and unclassified information. The Office of the Chief Information Officer and SEPS developed policy based on authority derived from DOJ Order 2640.2E.

The Department's Chief Information Officer issued 18 *Information Technology Security Standards* for DOJ systems that process classified and unclassified information. The 18th standard, titled *Information Technology Security Standard, Management Controls*, *1.6 Classified Laptop and Standalone Computers Security Policy* (Standard 1.6), established uniform IT security management controls for classified laptop (portable) and standalone computers storing, processing, or transmitting National Security Information in the DOJ.

Policy issued by SEPS, titled the *Security Program Operating Manual* (SPOM), provides guidance for the safeguarding of classified information. The SPOM applies to classified information, the facilities authorized to store the information, security controls, and security clearance requirements for employees.

---

[2] The CNSS is the policy making body for all issues concerning the security of national security systems for the federal government. See Appendix II for a list of the voting members on the committee.

[3] Sensitive Compartmented Information is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence.

Audit Results

Our audit disclosed areas where improvements can be made to the current DOJ policy and practices relating to storing, processing, or transmitting classified information on portable computers. Specifically, we found Standard 1.6 includes inappropriate and confusing references and is incomplete in providing guidance and instructions. Further, we identified innovative practices to improve the use of portable computers for processing classified information while adequately safeguarding classified information.

Standard 1.6

We identified three areas of concern with DOJ policy Standard 1.6. First, although Standard 1.6 was written to address the processing of classified information, it uses references to policies that do not apply to portable or standalone computers that process, store, or transmit classified information. For example, Standard 1.6 refers to Office of Management and Budget *Circular A-130*, Revised, (Transmittal Memorandum No. 4; Subject: Management of Federal Information Resources); *Federal Information Processing Standards Publication 197, Advanced Encryption Standard* (FIPS 197); DOJ Order 2620.7, *Control and Protection of Limited Official Use Information*; 5 CFR Part 930, *Training Requirement for the Computer Security Act*; and 18 U.S.C. 2510, *Electronic Communications Privacy Act*. These documents relate to unclassified information. Policies for systems that process unclassified information have no authority over systems that store, process, or transmit classified information and, therefore, should be omitted from the guidance. Inclusion of inappropriate references in this Standard may confuse employees and lead to implementation of incorrect practices.

Second, Standard 1.6 does not address the systems that process Classified National Security Information and Sensitive Compartmented Information separately, as those systems are subject to policies that are derived from different authorities. Despite unique and specific guidance regarding Classified National Security Information and Sensitive Compartmented Information, stipulated by Presidential delegated government-wide authorities, Standard 1.6 does not differentiate between the two types of information or provide separate processing requirements for information classified under these distinct designations.

Third, we found that Standard 1.6 includes incomplete guidance and instructions. For example, it states that classified portable computers may not be connected to external systems, networks, or communication devices. However, the Deputy Chief Information Officer informed us that classified portable computers can be connected to classified networks if the approval

to do so is documented in the security plan for the certification and accreditation of the network. Standard 1.6 needs to be updated to clarify this exception.

Another example of incomplete guidance and instructions in Standard 1.6 concerns two of its attachments. Attachment 2 (Security Acknowledgment Statement for System Administrators) is not referred to in the body of the policy; therefore its intended purpose and usage is unclear. Attachment 5 (Sample Classified Computer Usage Log) also is not referred to in the body of the policy and contains no instructions for its completion or the retention period for the log.

Increasing Efficiency When Processing Classified Information in Portable Computers

Our audit also identified several ways for the Department to more efficiently and economically store, process, and transmit classified information in portable computers.

Removable Hard Drives. Standard 1.6 allows for the use of portable computers with removable hard drives when processing classified information. However, it does not explicitly authorize the use of two hard drives, one for classified information and one for unclassified information, in a single portable computer. We asked officials from the EOUSA, DEA, and FBI: (1) if their agencies authorized the use of portable computers with removable hard drives, one to process classified and another to process unclassified on the same computer, and (2) if not, whether they would consider the feature worthwhile. Officials from all three agencies responded negatively to the first question. The responses to the second question varied between the agencies. EOUSA responded that the issue does come up and it would probably be worthwhile to pursue as long as users understand the applicable security requirements. The DEA responded that while the feature would have fiscal advantages, the risk of procedural errors such as forgetting to exchange removable hard drives for the appropriate type of information processing, could negate the utility of interchanging hard drives. The FBI responded that the feature could be worthwhile, but it would need to evaluate any proposed use of removable hard drives based on the operational need, technical configuration of the system, and other mitigating factors through the certification and accreditation process.

We also contacted agencies outside of the DOJ to discuss their policies with respect to removable hard drives.[4] Except for the Department of

[4] The CIA, the National Security Agency, the National Reconnaissance Office, and the Department of Energy.

Energy, these agencies process both classified and unclassified information by using portable computers with two separate removable hard drives — one hard drive for processing classified information and the other for processing unclassified information.[5]

In our view, the use of removable hard drives is an area that the Department should consider.

Type Accreditations. The concept of type accreditations, defined by the Chief Information Officer in Standard 1.6 for portable and standalone computers, is an abbreviated accreditation process for classified portable and standalone computers that can be used in lieu of a full certification and accreditation process.[6] The Chief Information Officer developed this approach to limit the unnecessary duplication of the full certification and accreditation requirements. However, Standard 1.6 does not document the process that DOJ components should use to request type accreditations for new computer configurations.

Encryption. Encryption of the hard drive is a safeguard required by the Committee on National Security Systems that can help protect classified information from unauthorized use if a portable computer or hard drive is lost or stolen. Encryption involves a set of mathematically expressed rules for rendering data unintelligible to an unauthorized user. Standard 1.6 does not explicitly require the use of the encryption standard specified by the Committee on National Security Systems.

Limited Data on Hard Drives.

or stolen. If such devices were installed, a lost or stolen computer could more easily be located.

Recommendations

We made 12 recommendations to assist the Department in improving the storing, processing, and transmitting of classified information on portable computers. For example, we recommend a revision of Standard 1.6 in order to remove any references to statute, policy, or procedures that are not applicable to processing classified information, indicate what policy applies when classified portable computers are allowed to be connected to classified networks, and address systems that process Classified National Security Information independently from those that process Sensitive Compartmented Information.

We also recommend that the Department consider the use of removable hard drives for processing both classified and unclassified information on the same portable computer by using two separate removable hard drives. This would require that the hard drive become the classifiable device instead of the portable computer and that appropriate security safeguards be developed. Additional recommendations relate to the use of encryption, tracking devices, and the sending of alerts to systems administrators when classified devices are improperly connected to the Internet.

TABLE OF CONTENTS

Page

INTRODUCTION 1
Government-wide Policy on the Certification and Accreditation of IT Systems 2
DOJ Policy 4

FINDINGS AND RECOMMENDATIONS 7

1. STANDARD 1.6 HAS INAPPROPRIATE REFERENCES AND IS INCOMPLETE 7
Inappropriate References in Standard 1.6 8
Separate Authority Governing Classified National Security Information and Sensitive Compartmented Information 9
Incomplete Guidance and Instructions 10
Conclusion 11
Recommendations 11

2. INCREASING EFFICIENCY WHEN PROCESSING CLASSIFIED INFORMATION ON PORTABLE COMPUTERS 13
Removable Hard Drives and Operating System 13
Type Accreditations 16
Safeguards for Lost or Stolen Computers 16
Labeling Requirements for Classified Information Media 18
Recommendations 18

STATEMENT ON INTERNAL CONTROLS 20

APPENDICES 21
Appendix I - Objectives, Scope, and Methodology 21
Appendix II - Voting Members of the Committee on National Security Systems 22
Appendix III - Classified Laptop and Standalone Computers Security Policy, Standard 1.6 23
Appendix IV - Chief Information Officer's Response to the Audit Recommendations 48
Appendix V - Office of the Inspector General, Audit Division, Analysis and Summary of Actions Necessary to Close Report 53

PROCESSING CLASSIFIED INFORMATION ON PORTABLE COMPUTERS IN THE DEPARTMENT OF JUSTICE

INTRODUCTION

This Office of the Inspector General audit examines the policies and practices in the Department of Justice (DOJ or Department) for the processing of classified information in portable computers. Our approach for conducting this audit included: (1) interviewing officials from within and outside the Department about classified portable computing policies and practices and (2) examining government-wide and DOJ policy related to processing classified information.

During our initial discussions with the Department's Deputy Chief Information Officer and the Assistant Director of the Security and Emergency Planning Staff (SEPS), they identified DOJ components that process classified information using portable computers. We selected the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the Executive Office for United States Attorneys (EOUSA) to examine the use of portable computers for processing classified information.

We extended our interviews beyond the DOJ to determine how other federal agencies address the storing and processing of classified information using portable computers. We met with staff from SEPS and the Chief Information Officer's office and discussed their knowledge of other federal agencies that process classified information on portable computers. Based on their input, we interviewed Information Technology (IT) and security personnel from the National Security Agency, the Central Intelligence Agency (CIA), and the Department of Energy. Based on input from the CIA, we also contacted the National Reconnaissance Office within the Department of Defense. (See Appendix I for additional information on our objectives, scope, and methodology.)

Our original intention was to examine the policies and practices in the DOJ for the processing of classified information on portable computers. However, IT and security staff informed us that we should also review government-wide policy that applies to all IT systems, whether they process classified or unclassified information. Therefore, our audit includes a review of the following government-wide policy (National Institute of Standards and Technology, *Special Publication 800-37*; Committee on National Security Systems, *National Information Assurance Certification and Accreditation Process*; and the Director of Central Intelligence Directives, *DCID 6/3*) that

requires all computer systems be certified before they can be placed in operation.

Government-wide Policy on the Certification and Accreditation of IT Systems

The certification of an IT system involves a comprehensive evaluation of the technical and non-technical security features and other safeguards in place on a system. The certification is made as part of and in support of the accreditation process. The certification process validates that appropriate safeguards have been implemented on the system. The process culminates in the accreditation of the system (permission for the system to operate).

During our research, we identified the organizations that have the responsibility to develop government-wide policy related to the certification and accreditation of IT systems. The policies cover all IT systems, including portable computers. As detailed in the following table, three organizations have the responsibility to develop policy for the certification and accreditation of all IT systems.

Government-wide Certification and Accreditation Authority

Organization	Type of Information	Source of Authority
National Institute of Standards and Technology (NIST)	Unclassified	*Federal Information Security Management Act* (FISMA) (December 17, 2002)
Committee on National Security Systems (CNSS)[7]	Classified National Security Information (CNSI)	Executive Order 13231 (as amended September 17, 2003)
Central Intelligence Agency (CIA)	Sensitive Compartmented Information (SCI)	Executive Order 12333 (as amended August 27, 2004) and Executive Order 12958 (as amended March 25, 2003)

The *Federal Information Security Management Act* (FISMA) delegates policy development and oversight to the National Institute of Standards and Technology (NIST) for information systems other than national security systems. Certification and accreditation procedures for systems other than

[7] See Appendix II for a complete list of the voting members of the Committee on National Security Systems.

national security systems — unclassified systems (systems that process only unclassified information) — are documented in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*

To separate unclassified from classified systems, NIST Special Publication 800-59 includes six questions designed to determine whether the system meets the definition of a national security system. According to the publication, "In order for a system to be designated a national security system, one of the following questions must be answered in the affirmative:"

- Does the function, operation, or use of the system involve intelligence activities?
- Does the function, operation, or use of the system involve cryptologic activities related to national security?
- Does the function, operation, or use of the system involve command and control of military forces?
- Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?
- Is the system critical to the direct fulfillment of military or intelligence missions?
- Does the system store, process, or communicate classified information?

Based on the NIST policy, any system that stores, processes, or communicates classified information is a national security system and falls under the jurisdiction of the Committee on National Security Systems.

Executive Order 13231, *Critical Infrastructure Protection,* identifies the government-wide committees that develop policy for the protection of information systems. Based on Executive Order 13231, the Committee on National Security Systems is responsible for policy over national security systems. The Committee on National Security Systems has documented procedures for the certification and accreditation of national security systems in the *National Information Assurance Certification and Accreditation Process* (NIACAP).

National security systems store, process, or transmit classified information as defined by Executive Order 12958, *Classified National*

Security Information. The Order defines three levels of Classified National Security Information:

- Top Secret — classified information where the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security;

- Secret — classified information where the unauthorized disclosure could reasonably be expected to cause serious damage to national security; and

- Confidential — classified information where the unauthorized disclosure could reasonably be expected to cause damage to national security.

Executive Order 12333, *United States Intelligence Activities*, requires that the Director of Central Intelligence, "Ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products." In addition, Executive Order 12958, Section 4.3, delegates to the Director of Central Intelligence authority over special access programs pertaining to intelligence activities. Further, certification and accreditation of systems used to process intelligence information, referred to as Sensitive Compartmented Information, is documented in *Director of Central Intelligence Directive (DCID) 6/3*.[8]

The policies developed by the Committee on National Security Systems and the CIA take precedence over the standards developed by the Department's Chief Information Officer for national security systems.

DOJ Policy

When necessary, DOJ employees store, process, and transmit classified information using portable computers. Employees may also process sensitive but unclassified information, send and receive e-mail, and obtain research data from the Internet on portable computers. Currently, employees who process both classified and unclassified information must utilize two separate portable computers in order to accomplish their

[8] Sensitive Compartmented Information is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence.

assignments. Carrying two portable computers is necessary because the current DOJ policy does not explicitly authorize the use of two hard drives, one for classified information and one for unclassified information, in a single portable computer.

DOJ Order 2640.2E, titled *Information Technology Security*, establishes uniform policy, responsibilities, and authorities for the implementation and protection of DOJ's IT systems that store, process, or transmit classified and unclassified information. The Assistant Director of SEPS and the Deputy Chief Information Officer described the distinction between the responsibilities of the two offices as the Chief Information Officer being responsible for security of classified and unclassified IT systems and SEPS being responsible for security of the classified information.

The Department's Chief Information Officer issued 17 *Information Technology Security Standards* between December 4, 2003, and January 30, 2004, for DOJ systems that process classified and unclassified information. In addition, an 18th standard was issued on August 19, 2004, titled *Information Technology Security Standard, Management Controls*, *1.6 Classified Laptop and Standalone Computers Security Policy* (Standard 1.6). Standard 1.6 established uniform information technology security management controls for laptop (portable) and standalone computers storing, processing, or transmitting National Security Information in the DOJ.[9] All IT systems in the DOJ that process classified information must be certified and accredited in accordance with standards established by the Department's Chief Information Officer before the system can be used.

Policy issued by SEPS, titled *Security Program Operating Manual* (SPOM), revised November 5, 2004, provides guidance for the safeguarding of classified information. The SPOM applies to classified information, security controls, security clearance requirements for employees, and the facilities authorized to store the information.

Classified National Security Information cannot be processed in public areas or while being transported. According to the SPOM and DCID 6/9, such information can be processed in only four specific types of facilities — a Sensitive Compartmented Information Facility (SCIF), a Temporary Secure Working Area, an Open Storage Area, or a Restricted Area.

[9] During this audit, we analyzed a draft copy of Standard 1.6 (Standard 1.3, version 0.5), issued March 31, 2004, by the Office of the Chief Information Officer. We received a copy of the final version of Standard 1.6 on September 8, 2004.

A SCIF is an accredited area, room, group of rooms, buildings, or installation where Sensitive Compartmented Information may be stored, used, discussed, and electronically processed. A Temporary Secure Working Area is a space where Sensitive Compartmented Information may be handled, discussed, or processed, but should not be stored. SEPS oversees design and security of SCIFs and Temporary Secure Working Areas within the DOJ, with the exception of the FBI who is responsible for the design and security of SCIFs and Temporary Secure Working areas under its jurisdiction.

An Open Storage Area is used when the volume or bulk of classified material is such that the use of security containers is not practical. When a component determines that an Open Storage Area is necessary, its location and construction must be approved by the Department Security Officer. A Restricted Area can be established when it is necessary to control access to classified material in an area not approved for open storage. All classified material must be secured during non-working hours in approved security containers or vaults. Open Storage Areas and Restricted Areas are accredited by SEPS for the DOJ, with the exception of the FBI who is responsible for the design and security of Open Storage Areas and Restricted Areas under its jurisdiction.

In Restricted Areas or Temporary Secured Working Areas, the user must maintain constant possession of the hard drive containing classified information, or it must be locked in an approved security container. Further, if the hard drive cannot be removed from the computer, the computer must be disconnected from its peripheral devices, i.e., a mouse, monitor, keyboard, and printer, and locked in an approved security container when not in use.

FINDINGS AND RECOMMENDATIONS

1. STANDARD 1.6 HAS INAPPROPRIATE REFERENCES AND IS INCOMPLETE

Standard 1.6 uses references to policies that were written for unclassified IT systems. Standard 1.6 does not address systems that process Classified National Security Information separately from systems that process Sensitive Compartmented Information. Furthermore, Standard 1.6 provides incomplete guidance and instruction for network connections, and two of its attachments are not referred to in the body of the policy. We recommend that Standard 1.6 be revised to reduce the difficulty that DOJ components may have when attempting to comply with Standard 1.6.

Standard 1.6 contains the following categories of specific requirements for laptops and standalone computers that store, process, or transmit National Security Information:

- Administrative Security
- Physical Security
- Personnel Security
- Identification and Authentication
- Audit Trail and Review
- Logical Access Control
- Password Management
- Software Security
- Telecommunications Security
- Media Security
- Continuity of Operations
- Incident Response
- Encryption

Standard 1.6 also contains seven attachments: a security acknowledgement statement for authorized end-users, a security acknowledgement statement for system administrators, hardware and software configurations of classified laptop and standalone computers, a list of acronyms, a sample classified computer usage log, a sample classified

computer maintenance log, and a classified laptop and standalone computer technical checklist (see Appendix III, pages 35-47 for specifics).

Our review of Standard 1.6 identified three primary areas of concern, discussed in greater detail below. Standard 1.6 uses references that apply to unclassified IT systems, does not address systems that process Classified National Security Information separately from systems that process Sensitive Compartmented Information, and provides incomplete guidance and instructions for several attachments.

Inappropriate References in Standard 1.6

Standard 1.6 uses references to policies that do not apply to portable or standalone computers that process, store, or transmit classified information (see Appendix III, page 29). The following five policy references used in Standard 1.6 do not apply to portable or standalone computers that process classified information:

- Office of Management and Budget *Circular A-130*, Revised, (Transmittal Memorandum No. 4; Subject: Management of Federal Information Resources) — This Circular discusses national security systems, but states in the section titled Applicability and Scope that, "Information classified for national security purposes should also be handled in accordance with the appropriate national security directives." Further, the Circular states, "The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451)." The *Clinger-Cohen Act* relates to the budget process for IT systems, not the processing of classified information.

- *Federal Information Processing Standards Publication 197, Advanced Encryption Standard* (FIPS 197) — FIPS 197 does not apply to classified systems. The Standard states, "This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection." Rather than referencing FIPS 197 for encryption of classified information on portable or standalone computers, the DOJ should reference the methods prescribed by the Committee on National Security Systems.

- DOJ Order 2620.7, *Control and Protection of Limited Official Use Information* — The subject of DOJ Order 2620.7 is control and protection of limited official use information. Therefore, it does not apply to classified systems, and the reference to this order should be deleted.

- 5 CFR Part 930, *Training Requirement for the Computer Security Act* — 5 CFR Part 930 does not apply to classified systems. The authority for the regulation, Public Law 100-235, is limited to sensitive but unclassified information. Standard 1.6 should instead refer to computer security training (IT Security Standard 2.8) and protection of classified information training (SPOM, Chapter 3).

- 18 U.S.C. 2510, *Electronic Communications Privacy Act* — This Act discusses the interception of wire, electronic, and oral communications. Standard 1.6 does not allow any type of telecommunications for portable or standalone computers processing classified information.

We believe the references that do not apply to portable or standalone computers that process classified information should be removed. Also, any instructions provided in Standard 1.6 that were derived from those incorrect references should be deleted from the document. The Assistant Director of SEPS concurred with our position that unclassified references should not be used in standards for storing, processing, or transmitting classified information.

Separate Authority Governing Classified National Security Information and Sensitive Compartmented Information

Standard 1.6 provides a uniform policy for portable and standalone computers that store, process, or transmit classified information (see Appendix III, page 25). However, there are two organizations outside the DOJ that have government-wide authority over the security of systems that store, process, or transmit classified information. The Committee on National Security Systems issued certification and accreditation policy for systems that process Classified National Security Information. Further, the CIA issued certification and accreditation policy for systems that process Sensitive Compartmented Information. Despite unique and specific guidance regarding Classified National Security Information and Sensitive Compartmented Information from these government-wide authorities, Standard 1.6 does not differentiate between the two or provide separate

processing requirements for information classified under these distinct designations.

We believe that Standard 1.6 should address the systems that process Classified National Security Information and Sensitive Compartmented Information separately, because those systems are subject to policies developed by two separate government-wide authorities. SEPS, a voting member of the Committee on National Security Systems for the Department of Justice (see Appendix II, page 22), agrees with our position.

Incomplete Guidance and Instructions

We found three areas, described below, where the guidance and instructions provided in Standard 1.6 are incomplete and therefore need revision.

Lack of Instructions for Network Connections. Section 3.1, states that, "No external systems, networks, or communications devices may be connected to classified laptop and standalone computers." (See Appendix III, pages 30 and 31.) However, the Deputy Chief Information Officer informed us that classified portable computers can be connected to classified networks if the approval to do so is documented in the security plan for the certification and accreditation of the applicable network. Based on that information, Standard 1.6 is not accurate regarding Department policy on the connection of portable computers to external systems, networks, or communication devices. In our opinion, Standard 1.6 should not provide a blanket prohibition, but should indicate what policies apply when classified laptop computers are authorized to be connected to classified networks.

No Explanation of Security Configuration Tests. We asked the Deputy Chief Information Officer why Attachment 2, entitled "Security Acknowledgement Statement for System Administrators" (see Appendix III, pages 37-39), requires that the System Administrator "make the computer(s) available for reviews of the security configuration by independent testers" and "ensure that the Certification Agent (CA) or a CA appointed agent validates system security at least annually." The Deputy Chief Information Officer stated that logistical and organizational issues concerning certification and independent testing are being negotiated. However, Attachment 2 is not referred to in the body of Standard 1.6. Therefore, the process for reviews of the security configuration by independent testers and a validation of system security by certification agents should be documented in the body of the policy.

No Instructions for Tracking Log. Attachment 5, "Sample Classified Computer Usage Log" (see Appendix III, page 44), has no instructions for completing the log. In addition, Standard 1.6 does not refer to the log or provide a retention period for the log. As written, either the end-user or the administrator must record every action taken on every document accessed, along with start and end times. As presented, we consider the log to be unduly burdensome and in need of revision. The Deputy Chief Information Officer explained that there is a need for a manual record of the total time an individual was logged onto the classified system. We understand the value of a tracking log, but the attachment will require modification in order to capture only the required information, and instructions will have to be prepared to inform the end-users and administrators about how to complete the log and for how long it should be retained. The Deputy Chief Information Officer indicated that this issue would be addressed in the next revision of Standard 1.6.

Conclusion

Standard 1.6 includes inaccurate and confusing references directed at unclassified systems, does not address systems that process Classified National Security Information separately from Sensitive Compartmented Information, and is incomplete in providing guidance and instructions. We believe that Standard 1.6 could be confusing to DOJ components and should be revised to correct these deficiencies.

Recommendations

We recommend that the Justice Management Division revise Standard 1.6 to:

1. Remove any references to statute, policy, or procedures that are not applicable to processing classified information.

2. Address systems in accordance with policy from the Committee on National Security Systems for Classified National Security Information independently from the Director of Central Intelligence Directives for Sensitive Compartmented Information.

3. Indicate what policy applies when classified portable computers are allowed to be connected to classified networks.

4. Refer to Attachment 2 (Security Acknowledgement Statement for System Administrators) in the body of the policy and delineate the

process for reviews of the security configuration by independent testers and validation of the system security by certification agents.

5. Refer to Attachment 5 (Sample Classified Computer Usage Log) in the body of the policy and provide written instructions for the preparation and retention of the log.

2. INCREASING EFFICIENCY WHEN PROCESSING CLASSIFIED INFORMATION ON PORTABLE COMPUTERS

The Department should consider modification of any practices for processing classified information on portable computers from those prescribed in Standard 1.6. We believe that the DOJ's Chief Information Officer should consider revising the policy to allow for a variety of innovative features and methods to enhance the ability of the DOJ to accomplish its mission, while adequately securing its classified information.

We met with four DOJ components (DEA, FBI, EOUSA, and Justice Management Division) and four outside agencies (CIA, National Security Agency, National Reconnaissance Office, and the Department of Energy) to determine how they address the storage of classified information using portable computers and to determine whether more effective practices are available to enhance security. All of the agencies contacted, with the exception of the DEA, store and process some of their classified information on portable computers.

From discussions with those interviewed and our review of Standard 1.6 and the SPOM, we identified four security policy enhancements we believe the Department should consider for classified portable computers. The following sections describe those enhancements.

Removable Hard Drives and Operating System

We asked officials from the EOUSA, DEA, and FBI: (1) if their agency authorized the use of portable computers with removable hard drives, one to process classified and another to process unclassified on the same computer, and (2) if not, whether they would consider the feature worthwhile. Officials from all three agencies responded negatively to the first question. The responses to the second question varied among the agencies. The EOUSA responded that the issue does come up and it would probably be worthwhile to pursue as long as users understand the applicable security requirements. The DEA responded that while the feature would have fiscal advantages, the risk of procedural errors such as forgetting to exchange removable hard drives for the appropriate type of processing, could negate the utility of

interchanging hard drives.[10] The FBI responded that the feature could be worthwhile, but it would need to evaluate any proposed use of removable hard drives based on the operational need, technical configuration of the system, and other mitigating factors through the certification and accreditation process.

Three of the four agencies we interviewed outside the DOJ process both classified and unclassified information on the same computer by using two separate removable hard drives — one hard drive for processing classified information and the other for processing unclassified information.[11]

We discussed the subject of removable hard drives with a major portable computer manufacturer who told us of at least two companies that sell 5-gigabyte (5,000 megabytes) removable hard drives. The drives are priced under $200 each. These drives are generally two inches wide by three inches long, weigh less than two ounces, and fit into any "Type II PC Card slot" in portable computers. As presented in the table below, we believe they have enough storage space for a multi-user operating system, application software, and a reasonable amount of space for processing classified information. The table illustrates one example of a portable computer's software configuration we believe would meet the needs of many of the DOJ's classified computer users. With the Chief Information Officer's approval, 5-gigabyte removable hard drives could be used on the DOJ's portable computers that process classified information. This computer configuration would allow both unclassified and classified information processing in the same portable computer.

Operating System and Application Software Minimum Requirements

Example of a Usable Software Configuration	Space Requirements
Microsoft XP Professional	230 megabytes
Microsoft Office Professional	600 megabytes
Data Encryption	15 megabytes
Virus Detection	16 megabytes
Sub Total	861 megabytes
Remaining Space	4,139 megabytes

Source: Software company websites.

[10] We believe that DEA's concern does not adequately consider that the SPOM requires computers to contain banners reminding users of the classification for the system. The SPOM states, "to avoid inadvertent compromises, removable hard drives used on IT systems for unclassified and classified processing will utilize desktop backgrounds that display classification banners at the top or bottom."

[11] The Department of Energy uses classified portable computers with removable hard drives but does not interchange an unclassified hard drive with the classified hard drive. The other three agencies are the CIA, the National Security Agency, and the Nat

Using removable hard drives offers advantages for portable computers. Without removable hard drives, a user may be required to carry two portable computers while on a traveling assignment — one for handling classified information, which requires it to be double-wrapped, and the other for processing unclassified information, connecting to the Internet, and viewing e-mail.[12] With removable hard drives, the user would be required to double wrap only the classified hard drive instead of the entire portable computer. In our opinion, a double-wrapped classified removable hard drive is an effective security enhancement, as it is easier to conceal and is less conspicuous due to its smaller size compared to a portable computer.

Although Standard 1.6 approves of removable hard drives (Appendix III, page 41), it does not specifically authorize the use of dual classified and unclassified hard drives in the same portable computer. Without removable hard drives, users processing classified information on a portable computer must disconnect all of the attached peripheral devices and secure the entire computer in an approved security container when it is to be left unattended. In contrast, with a removable hard drive a DOJ employee merely has to remove the classified hard drive and secure it, not the computer shell.

In order to enhance security of the classified information when using removable hard drives, system administrators must define user profiles within the operating system for classified portable computers. For example, IT security personnel at the National Reconnaissance Office and National Security Agency told us that a multi-user operating system, such as Microsoft Windows 2000 or XP, allows system administrators to define computer users' profiles and therefore restrict access to the computer's input/output ports. Specifically, the access to the unclassified drive when the removable classified hard drive is in use can be controlled by the definition of the user's profile. In addition, they also said that users' profiles can allow access to Internet connections when the classified hard drive is not in use.

In our view, the use of removable hard drives that can process both unclassified and classified information in the same computer shell is an area that the Department should consider.

[12] Double wrap — classified information must be "…enclosed in two opaque layers; both of which provide reasonable evidence of tampering and conceal the contents."

Type Accreditations

The concept of type accreditations, defined by the Chief Information Officer in Standard 1.6 for portable and standalone computers, is an abbreviated accreditation process for classified portable and standalone computers that can be used in lieu of a full certification and accreditation process (see Appendix III, page 30).[13] The Chief Information Officer developed this approach to limit the unnecessary duplication of the full certification and accreditation requirements. The Department's Assistant Director of SEPS stated that a type accreditation for classified portable and standalone computers is an acceptable procedure.

Standard 1.6, Attachment 3 (*Hardware and Software Configurations of Classified Laptop and Standalone Computers*), defines three specific types of computer configurations: classified laptop computers, classified standalone computers, and computers with removable hard drives (see Appendix III, pages 40-42). Each of the three specific types of computer configurations contains a list of recommended hardware configurations, mandatory hardware features, and software configurations.

We believe that Standard 1.6 should allow the DOJ components more flexibility in the design of portable and standalone computer systems. The Deputy Chief Information Officer informed us that flexibility is built into the type accreditation process. However, the process to obtain type accreditations for other configurations is not documented in Standard 1.6. A revised Standard 1.6 should document the process for DOJ components to follow when requesting computer configurations not specified in the Standard. Furthermore, Standard 1.6 should be written to allow the DOJ components flexibility to incorporate innovative safeguards that do not compromise security.

Safeguards for Lost or Stolen Computers

Additional effective safeguards for classified computers and hard drives may strengthen security by lowering the risk of unauthorized persons gaining access to classified information in the event a portable computer is lost or stolen.

For example, encryption of the hard drive is a safeguard that IT and security personnel believe can reasonably protect classified information from

[13] Accreditation of a system is the permission for an IT system to operate.

unauthorized use if a portable computer is lost or stolen.[14] As discussed on page 8, the Chief Information Officer's reference for encryption cites the *Federal Information Processing Standard Publication 197 — Advanced Encryption Standard* (Appendix III, page 29). Yet, FIPS 197 applies to unclassified systems, not classified systems, which is the focus of Standard 1.6. Further, the Committee on National Security Systems has a Presidential delegation for national security systems through Executive Order 13231. Therefore, we believe the Chief Information Officer should explicitly require the use of the encryption standard specified by the Committee on National Security Systems when defining DOJ standards.

In addition to encryption, we identified three security enhancements that the DOJ could use to protect classified information on portable computers. The following safeguards could help reduce the amount of damage or decrease the chances of unauthorized individuals gaining access to classified data in the event a portable computer or hard drive is lost or stolen:

- Reduce the risk of unauthorized access to classified information while the portable computer is in transit by limiting the amount of classified information on the hard drive to the minimum amount of information necessary to accomplish the mission. This safeguard, used by the National Security Agency, reduces the amount of damage that can occur if an unauthorized user gains access to the information.

- Program the computer's operating system to send a message to the system administrator if the computer is connected to the Internet. Connecting a classified computer to the Internet increases the risk that unauthorized users may obtain access to classified information. The National Reconnaissance Office uses this safeguard. Sending a warning message to a system administrator would allow a DOJ component to take steps to mitigate potential damage to national security in the event of a security breach.

- Install an electronic device on the portable computer that can track or locate the equipment using global positioning technology. If such a device were installed, the computer could be tracked and located if it was lost or stolen.

We believe that these security enhancements identified by IT and security personnel should be considered by the Chief Information Officer

[14] Encryption involves a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

when drafting policy for portable computers processing classified information.

Labeling Requirements for Classified Information Media

Current Department policy, in Chapter 8, Section 8-203, of the SPOM, specifically states, "Classification Markings (Labels) must be displayed on all components of an IT system that have the potential for retaining classified information." The IT and security staff we interviewed at the National Security Agency indicated that the shell of a portable computer does not retain any retrievable data after removal of the computer's hard drive containing the operating system. The National Security Agency staff further said that once a computer is powered down, all data in the random access memory is gone and cannot be retrieved, effectively sanitizing the computer shell. In our opinion, Standard 1.6 should specify that the shell does not remain classified after the classified hard drive is removed.

Using removable hard drives on classified portable computers would require creating a new label for the shell to indicate that the computer might contain classified information, but is also cleared to process unclassified information. Therefore, the SPOM should be revised to describe the markings for this type of equipment. The Assistant Director of SEPS agreed with our position on labeling the portable computer shell and indicated that the change to the labeling requirement would occur during the next SPOM revision.

Recommendations

We recommend that the Justice Management Division:

6. Consider the use of removable hard drives for processing both classified and unclassified information on the same portable computer by using two separate removable hard drives. This would require that the hard drive become the classifiable device instead of the portable computer and that appropriate security safeguards be developed.

7. Document the process that gives DOJ components the flexibility to incorporate safeguards through new type accreditations to protect classified computers from unauthorized access.

8. Adopt the encryption standard specified by the Committee on National Security Systems.

9. Consider enhancing security by writing policy to limit classified data on a hard drive to what is necessary to accomplish the mission.

10. Consider enhancing security by programming the computer to send a message to the system administrator if a computer with a classified hard drive is connected to the Internet.

11. Consider enhancing security by installing an electronic device on portable computers to track the equipment in the event it is lost or stolen.

12. Create a new label for portable computers that indicates the computer may contain classified information, but is also cleared to process unclassified information.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the Department of Justice's policy on the use of classified information in portable computers, we did not assess the Department's internal controls over the processing of classified information on portable computers. Our audit was more limited than would be necessary to express an opinion of the Department's internal control structure over classified information as a whole.

Reportable conditions, as defined by the *Government Auditing Standards*, involve matters coming to our attention relating to deficiencies that, in our judgment, could adversely affect the Department's controls over the processing of classified information in portable computers. During this audit, we did not identify any reportable conditions that could adversely affect the Department's controls over the processing of classified information.

This statement is intended solely for information purposes and use by the Department's management in their development of policy over the processing of classified information in portable computers. This usage restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to: (1) review the Department's policies and practices concerning the storage of classified information on portable computers, and (2) determine whether more effective practices could be adopted by the Department to enhance the ability to process classified information on portable computers while adequately safeguarding the information.

Our audit was performed in accordance with the *Government Auditing Standards* issued by the Comptroller General of the United States and included such tests as necessary using the performance auditing standards to accomplish the audit objectives stated above.

The scope of our audit included reviewing the DOJ Chief Information Officer's 18 *Information Technology Security Standards*; the DOJ's *Security Program Operating Manual*; Executive Orders 12333, 12958, and 13231; DOJ Orders 2640.2E and 2620.7; applicable sections of the *Federal Information Security Management Act of 2002*; applicable sections of the *Clinger-Cohen Act*; *NIST Publications* 800-37 and 800-59; applicable sections of the *National Information Assurance Certification and Accreditation Process* (NIACAP); Director *of Central Intelligence Directives*, DCIDs 6/3 and 6/9; *Federal Information Processing Standards Publication* 197; Office of Management and Budget *Circular A-130*; 5 CFR Part 930; and 18 U.S.C. 2510.

During our initial discussions with the Department's Deputy Chief Information Officer and the Assistant Director of the Security and Emergency Planning Staff, they identified DOJ components that process classified information using portable computers. Based on their recommendations of components that process classified information, we selected the Drug Enforcement Administration, the Federal Bureau of Investigation, and the Executive Office for United States Attorneys to discuss the use of portable computers for processing classified information.

We extended our interviews beyond the DOJ in order to determine how other federal agencies address the storing and processing of classified information using portable computers. Based on meetings with staff from SEPS and the Chief Information Officer's office, we interviewed IT and security personnel from the National Security Agency, the Central Intelligence Agency, and the Department of Energy. While conducting our interviews with staff at the Central Intelligence Agency, they recommended we also contact the National Reconnaissance Office within the Department of Defense.

APPENDIX II

VOTING MEMBERS OF THE COMMITTEE ON NATIONAL SECURITY SYSTEMS

The Acting Assistant Secretary of Defense for Networks and Information Integration who is also the Department of Defense Chief Information Officer currently chairs the quarterly meetings of the Committee on National Security Systems. The following list contains the representatives of the Committee on National Security Systems who have voting privileges.

Central Intelligence Agency
Defense Intelligence Agency
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation
Department of Treasury
Federal Bureau of Investigation
General Services Administration
National Security Agency
National Security Council
Office of Management and Budget
United States Air Force
United States Army
United States Joint Chiefs of Staff
United States Marine Corp
United States Navy

DEPARTMENT OF JUSTICE

INFORMATION TECHNOLOGY SECURITY

STANDARD

MANAGEMENT CONTROLS

1.6 CLASSIFIED LAPTOP AND STANDALONE COMPUTERS SECURITY POLICY

Version 1.1 August 19, 2004

Information Technology Security Staff
601 Pennsylvania Avenue NW Suite 230
Washington, DC 20530
202-353-3925

Table of Contents

1 Foreword 1
- 1.1 Feedback 2
- 1.2 Waivers/Exceptions 2

2 Overview 4
- 2.1 CONTENT SCOPE 4
- 2.2 POLICY 4
- 2.3 APPLICABILITY 4
- 2.4 REFERENCES 5

3 Requirements 5
- 3.1 Administrative Security 6
- 3.2 Physical Security 7
- 3.3 Personnel Security 7
- 3.4 Identification and Authentication 8
- 3.5 Audit Trail & Review 8
- 3.6 Logical Access Control 8
- 3.7 Password Management 8
- 3.8 Software Security 8
- 3.9 Telecommunications Security 9
- 3.10 Media Security 9
- 3.11 Continuity of Operations 9
- 3.12 Incident Response 9
- 3.13 Encryption 10

Attachment 1: Security Acknowledgement Statement for Authorized End-Users A-1
Attachment 2: Security Acknowledgement Statement for System Administrators A-3
Attachment 3: Hardware and Software Configurations of Classified laptop and standalone computers A-6
Attachment 4: List of Acronyms A-9
Attachment 5: Sample Classified Computer Usage Log A-10
Attachment 6: Sample Classified Computer Maintenance Log A-11
Attachment 7: Classified Laptop and Standalone Computer Technical Checklist A-12

1 FOREWORD

1. PURPOSE. This standard establishes uniform Information Technology Security Management Controls for laptop and standalone computers storing, processing, or transmitting National Security Information. This document contains directive materials to guide Department components in the development of appropriate controls and processes for these categories of systems.

2. SCOPE. The provisions of this standard apply to all Department Components, personnel, IT systems to include hardware, software, and media, facilities, and contractors acting on behalf of the Department. This standard also applies to any outside organizations, or their representatives, who are granted access to the Department's IT resources, such as other Federal agencies.

3. CANCELLATION. N/A

4. AUTHORITIES. The Deputy Chief Information Officer, IT Security, is responsible for providing security policy, guidance, implementation and oversight for IT systems. Questions or comments regarding this standard can be directed to the IT Security Staff.

Signed on August 19, 2004 by:

VANCE E. HITCH
Chief Information Officer
Department of Justice

1.1 FEEDBACK

Questions or comments concerning this document should be addressed to:

Deputy Director, Information Technology Security Staff
U.S. Department of Justice
601 Pennsylvania Avenue, NW
Suite 230
Washington, D.C. 20530
202-353-3925

1.2 WAIVERS/EXCEPTIONS

If the minimum requirements cannot be met, organizations shall request a waiver. Waivers or exceptions to individual Department standards shall be obtained by submitting, in writing to the Department of Justice Chief Information Officer (CIO), detailed information stating business, technical, or other issues associated with implementing the standards and the alternative countermeasures that will be put in place to ensure that this standard is being enforced. An action plan shall accompany the request which states how and when existing deficiencies or non-compliance will be mitigated or resolved.

Document History

Version #	Date	Description of Change	Author
0.1	March 17, 2004	Initial Draft.	John Wyatt
0.2	March 18, 2004	Minor corrections and additions.	John Wyatt
0.3	March 26, 2004	Changes to address comments to date from ITSS	John Wyatt
0.4	March 30, 2004	Changes to address more comments from ITSS	John Wyatt
0.5	March 31, 2004	Changes to address more comments from ITSS	John Wyatt
0.7	April 20, 2004	Changes to address more comments from ITSS	John Wyatt
1.0	July 30, 2004	Changes to address more comments from Components and ITSS	John Wyatt
1.1	August 19, 2004	Changes to address more comments from SEPS and ITSS	John Wyatt

2 OVERVIEW

2.1 CONTENT SCOPE

This document assigns responsibilities and addresses the information security policies for ensuring the confidentiality, integrity, and availability of Classified Laptop Computers and Classified Standalone Computers in the Department of Justice.

2.2 POLICY

Department policy in this area is provided by DOJ Order 2640.2E or its successors. This DOJ Order states: "Laptops and mobile computing devices are not authorized to process or store classified information unless approved in writing by the DSO and Department CIO. The Department CIO will issue standards for devices authorized for such use and will coordinate authorized standards with the DSO." In support of this policy, this standard contains the requirements for laptop computers that process or store classified information. In addition, this standard contains requirements for standalone computers that process or store classified information.

Consistent with the definitions used in the National Information Assurance Glossary and the National Information Assurance Certification and Accreditation Process (NIACAP), the Information Security Policy for a system is defined as "The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information." This policy draws from and supplements requirements contained in DOJ Order 2640.2E, the other DOJ IT Security Standards, the DOJ Security Program Operating Manual (SPOM), and other applicable national policies, federal laws, directives, regulations, rules and practices. In the event of a conflict between requirements contained herein and those in the reference documents, such conflicts should be brought to the attention of the DOJ Information Technology Security Staff for resolution.

All Government employees and contractor personnel will adhere to the DOJ SPOM and other applicable information security policies and procedures during all activities associated with the processing of such information on classified laptop computers and classified standalone computers. All information technology system components and media that process, store, or otherwise handle classified information must also be protected in accordance with the SPOM.

2.3 APPLICABILITY

This document applies to the implementation, management, administrative, maintenance, and end user personnel and facilities throughout the life cycle of each classified laptop computer and classified stand-alone computer.

2.4 REFERENCES

DOJ 2640.2E	DOJ Order Regarding Information Technology Security
DOJ 2620.7	Control and Protection of Limited Official Use Information
DOJ/SPOM	Security Program Operating Manual
FIPS 197	Advanced Encryption Standard (AES)
DCID 6/3	Protecting Sensitive Compartmented Information Within Information Systems
NSTISSI No. 1000	National Information Assurance Certification and Accreditation Process (NIACAP)
NTISSAM COMPUSEC/1-87	Advisory Memorandum on Office Automation Security Guideline
OMB Circular A-130	Management of Federal Information Resources
5 CFR Part 930	Training Requirement for the Computer Security Act
18 U.S.C. 2510	Electronic Communications Privacy Act
95 U.S.C. 552a	Privacy Act of 1987
DOJ ITS Standards	ITS Standard 1.1 Risk Management
	ITS Standard 1.2 Review Security Controls
	ITS Standard 1.3 Security Planning
	ITS Standard 1.4 Certification and Accreditation
	ITS Standard 1.5 System Security Plan
	ITS Standard 2.1 Personnel IT Security
	ITS Standard 2.2 Physical & Environmental IT Security
	ITS Standard 2.3 Production Input Output IT Security
	ITS Standard 2.4 Contingency Planning
	ITS Standard 2.5 System Maintenance
	ITS Standard 2.6 Data Integrity
	ITS Standard 2.7 Security Documentation
	ITS Standard 2.8 Security Awareness Training Education
	ITS Standard 2.9 Incident Response and Reporting
	ITS Standard 3.1 Identification and Authentication
	ITS Standard 3.2 Logical Access Control
	ITS Standard 3.3 Accountability and Audit.

3 REQUIREMENTS

The security policies to which classified laptop and standalone computers are subject have been developed to ensure the safe and secure operation of those computers. They are based on the minimum DOJ requirements mandated by DOJ Order 2640.2E, the DOJ Security Program Operating Manual (SPOM), the Office of Management and Budget Circular A-130, Appendix III,

Management of Federal Information Resources, the National Information Assurance Certification and Accreditation Process (NIACAP), and the Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*. In addition, all policies that are identified in the DOJ IT Security Standards apply to the classified laptop and standalone computers. Additional specific requirements for classified laptop and standalone computers, discussed below, are in the following categories:

- Administrative Security
- Physical Security
- Personnel Security
- Identification and Authentication
- Audit Trail & Review
- Logical Access Control
- Password Management
- Software Security
- Telecommunications Security
- Media Security
- Continuity of Operations
- Incident Response
- Encryption.

Specific technical requirements that apply to classified laptop and standalone computers are contained in the Attachment 3, Hardware and Software Configurations of Classified Personal Computers.

In addition, each classified laptop and standalone computer must be certified and accredited prior to use and re-certified and re-accredited every three years or whenever a major system change occurs. To limit the unnecessary duplication of certification and accreditation activities, the Justice Management Division performed a "type accreditation" for classified laptop and standalone computers. Components are encouraged to implement computers consistent with the type accreditation. Information regarding the "type accreditation" for classified laptop and standalone computers can be obtained from the Certification and Accreditation Help Desk at 202-353-3925.

3.1 ADMINISTRATIVE SECURITY

Administrative security pertains to the implementation of a risk management program. The following policies apply to the management of classified laptop and standalone computers:

- Each classified laptop and standalone computer will operate in either the Dedicated mode or the System High mode (as defined in the Security Program Operating Manual).

- ISSOs and SAs should follow the recommended process in Attachment 7 or a similar, locally generated, process to configure classified computers.
- No external systems, networks, or communications devices may be connected to classified laptop and standalone computers. (Classified computers that are intended to connect to classified computer networks are beyond the scope of this policy.)
- Wireless peripherals and wireless communications capabilities shall NOT be used with the classified computers that are supported by this security policy.
- The Certification Official will collect and maintain an inventory of all classified computers that are supported by this security policy.

3.2 PHYSICAL SECURITY

Physical security encompasses the measures taken to protect classified laptop and standalone computers against threats associated with the physical environment. The following physical security policies apply:

- Classified information SHALL ONLY be processed at approved U.S. Government facilities or approved contractor facilities.
- When not in use, classified laptop computers must be stored in approved security containers or in office areas approved for open storage commensurate with the classification level of the computers.
- Classified standalone computers with fixed hard disks can only be placed and used in office areas approved for open storage commensurate with the classification level of the computers.
- When not in use, removable classified hard disks as well as all media must be stored commensurate with the classification level of the computers.
- SCI computers can only be stored in a Sensitive Compartmented Information Facility (SCIF)
- Classified non-SCI systems can only be stored in an approved security container or in an office area approved for the open storage of classified information

3.3 PERSONNEL SECURITY

Personnel security pertains to staffing positions that interact with information systems and providing security awareness and training to the incumbents in these positions. The following policies apply to classified laptop and standalone computers:

- All personnel with access to classified information will receive background checks commensurate with the sensitivity of their positions.
- All persons with access to classified laptop and standalone computers will receive initial and annual security awareness training.

- All personnel using classified laptop and standalone computers shall possess a security clearance equal to or higher than the classification level of the information stored on the computers.

3.4 IDENTIFICATION AND AUTHENTICATION

The purpose of authentication is to provide for the reliable and proven identification of the user of the classified laptop and standalone computer. The following additional requirement applies:

- A separate and unique user identifier will be assigned to each person who has access to the classified laptop and standalone computer. This identifier will be authenticated using a password authentication mechanism.

3.5 AUDIT TRAIL & REVIEW

An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of a sequence of activities performed on a computer by one or more End Users or System Administrators. The classified laptop and standalone computer will meet all audit requirements promulgated in the ITS Standard 3.3, Accountability and Audit.

3.6 LOGICAL ACCESS CONTROL

Logical access controls provide a technical means to control user access to information and system resources. They control what information users can access, the programs they can run and the modifications they can make. The requirements for logical access control for laptop and standalone computers is contained in ITS Standard 3.2, Logical Access Control.

3.7 PASSWORD MANAGEMENT

Password management includes the generation, issuance, and control of the passwords that support authentication. Specific password management requirements are contained in ITS Standard 3.1, Identification and Authentication.

3.8 SOFTWARE SECURITY

The following policies apply to the installation and configuration of operating system and application software on the classified computer systems:

- Executable software will be identified in the system security plan and protected from unauthorized modification.

- A process to evaluate, test, and apply vendor-supplied patches, program fixes, and updates must be available. The process shall include a provision to expedite the application of high risk/high impact security-related patches. (This process will be complicated by the lack of network connectivity for classified laptop and standalone computers.)

3.9 TELECOMMUNICATIONS SECURITY

Telecommunications security is concerned with the protection of data during transmission. As currently defined, there will be no telecommunications capability for the classified laptop and standalone computers.

3.10 MEDIA SECURITY

The following policies apply to the marking and disposition of tapes, diskettes, hard drives, printouts, or any other media containing classified information:

- Any media containing classified information will be marked with its classification and other identifying information based on requirements contained in section 8-203 of the DOJ Security Program Operating Manual. (Media labels will be color-coded depending on the classification of the information contained on the media as specified in DCID 6/3.)
- Prior to release or disposal, electronic media containing classified data must be sanitized in accordance with section 8-207 of the DOJ Security Program Operating Manual, Disposition of Computer Media.

3.11 CONTINUITY OF OPERATIONS

The continuation of critical missions and business functions in the event of disruptions is assured by preparing in advance for contingencies and disasters. The ISSO, ISSM, and SA for each classified laptop and standalone computer should establish a contingency plan for the computer. The contingency plans for classified laptop and standalone computers shall be consistent with ITS Standard 2.4, Contingency Planning. In addition, any off-site storage facility must be approved for the storage of classified information and media.

3.12 INCIDENT RESPONSE

An information system incident is an unexpected, unplanned event that could have a negative impact on information technology resources. It requires immediate action to prevent further negative impacts. It may be an event that violates security policies or one that circumvents security mechanisms (e.g., intrusions, malicious software). Incident response for the classified

laptop and standalone computers shall be consistent with ITS Standard 2.9, Incident Response and Reporting and the SPOM. The incident response plan for the classified laptop and standalone computers provides for the handling of incidents via each component's standard incident reporting and response procedures.

3.13 ENCRYPTION

Encryption of the hard drive is performed on classified computer systems to protect against access by unauthorized persons (i.e., people without the requisite clearance and need-to-know). However, the software encryption technology currently employed on the DOJ classified laptop and standalone computers is not robust enough to protect classified information from exploitation by a well-funded and skilled adversary who has physical access to the computer or the data contained on the computer. Therefore, even though the information on the hard disks is encrypted, the computer must be protected as a classified item. The following requirements apply to the encryption process used to protect information on the hard disks of classified laptop and standalone computers:

- All information shall be encrypted using an ITSS-approved encryption software package.
- Passwords, access devices, and cryptographic keys associated with the encryption process must be handled as classified information.

When a classified computer system is provided to a defense attorney, at the discretion of the U.S. Attorney, it is acceptable to not implement the ITSS-approved encryption package.

ATTACHMENT 1: SECURITY ACKNOWLEDGEMENT STATEMENT FOR AUTHORIZED END-USERS

I understand that as an authorized user of a classified laptop and standalone computer, it is my responsibility to comply with all security measures necessary to prevent the unauthorized disclosure, modification, or destruction of information and the unauthorized modification or loss of control of a classified laptop and standalone computer.

I understand that the computer to which I will have access has been specially configured for classified processing based on guidelines from the DOJ Information Technology Security Staff (ITSS). I acknowledge that the configuration of this computer is subject to change and that upgrades to the configuration of this computer may occur to better satisfy requirements for classified processing. I agree to make this computer available upon reasonable notice to have the configuration altered by representatives of the DOJ ITSS. I agree to comply with the following Rules of Behavior that apply to authorized end-users of classified laptop and standalone computers:

1. Protect and safeguard information in accordance with the applicable Department practices and procedures including the DOJ Security Program Operating Manual.
2. Complete computer security awareness training annually.
3. Operate the computer only in those areas approved for the classification level of the computer unless specific authorization has been received from the Information System Security Officer to operate the computer in other areas.
4. Store the computer or the removable hard disk in an approved security container (or in a facility approved for open storage) when it is not in use.
5. Never remove the computer from cleared DOJ facilities without specific approval of the Information System Security Officer and the Security Program Manager.
6. Sign all logs, forms, and receipts as required.
7. Properly mark the classification of each document and section in accordance with the applicable DOJ and program classification guides.
8. Protect all media used on the computer by properly classifying, labeling, controlling, transmitting, and destroying it in accordance with security requirements.
9. Protect all hard copy produced at the highest classification level of system approval until reviewed for proper classification and control.
10. Notify the Information System Security Officer when access to the computer is no longer needed (e.g., transfer, termination, leave of absence, or for any period of extended non-use).
11. Choose a password in compliance with DOJ password policies and change that password as required by the password policies. In addition, use a different password than is used on other DOJ systems.

12. Protect the password as classified information at the level of classification authorized for the computer.
13. Ensure compliance with software and copyright laws.
14. Obtain permission from the Information System Security Officer, before changing any of configurations and settings of the operating system and security-related software.
15. Never install any software without the explicit approval of the Information System Security Officer.
16. Unless authorized by the Information System Security Officer, never add, modify, or remove hardware accessories to the computer.
17. Unless authorized by the Information System Security Officer, never connect any peripherals (e.g., printers) or networks to the computer.
18. Unless authorized by the Information System Security Officer, never access the internal components of the computer.
19. Make the computer available at any time to the Information System Security Officer for inspection and review of audit logs.
20. Make the computer available at any time to the System Administrator for the installation of patches and other system administration activities.
21. Never circumvent the security mechanisms used on and by the computer.
22. Unless authorized by the Information System Security Officer, never test the capabilities of the security control software that is installed on the computer.
23. Unless authorized by the Information System Security Officer, never attempt to access any electronic audit trails that may exist on the computer.
24. Immediately report, to the Information System Security Officer, any evidence of tampering with the computer.

I understand that these Rules of Behavior establish standards of actions in recognition of the fact that knowledgeable users are the foundation of a successful security program, and that non-compliance to these rules will be enforced through sanctions commensurate with the level of infraction. Administrative actions due to failure to follow these Rules of Behavior may range from a verbal or written warning, removal of system access for specific period of time, reassignment to other duties, to termination, depending on the severity of the violation. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

_____ _____

Printed Name of User Date

_____

Signature

ATTACHMENT 2: SECURITY ACKNOWLEDGEMENT STATEMENT FOR SYSTEM ADMINISTRATORS

I understand that as an authorized system administrator of classified laptop and standalone computers, it is my responsibility to comply with all security measures necessary to prevent the unauthorized disclosure, modification, or destruction of information and the unauthorized modification or loss of control of a classified laptop and standalone computer.

I understand that the computers to which I will have access have been, or will be, specially configured for classified processing based on guidelines from the DOJ Information Technology Security Staff (ITSS). I agree to properly implement guidelines from the ITSS in a timely manner on classified computers. I acknowledge that the configuration of the computer(s) is subject to change and that upgrades to the configuration of the computer(s) may occur to better satisfy requirements for classified processing. I agree to make the computer(s) available upon reasonable notice to have the configuration altered by representatives of the DOJ ITSS; or, if so directed, to make changes to the computer(s) consistent with guidance from DOJ Order 2640.2E, the IT Security Standards and directives from the ITSS.

I agree to comply with the following Rules of Behavior that apply to authorized system administrators of classified laptop and standalone computers:

1. Ensure that the Certification Agent (CA) or a CA appointed agent validates system security at least annually.
2. Protect and safeguard information in accordance with the applicable Department practices and procedures including the DOJ Security Program Operating Manual.
3. Make the computer(s) available for reviews of the security configuration by independent testers.
4. Complete computer security awareness training annually.
5. Operate the computer(s) only in those areas approved for the classification level of the computer(s) unless specific authorization has been received from the Information System Security Officer to operate the computer(s) in other areas.
6. Store the computer or the removable hard disk in an approved security container (or in a facility approved for open storage) when it is not in use.
7. Never remove the computer(s) from cleared DOJ facilities without specific approval of the Information System Security Officer and the Security Program Manager.
8. Sign all logs, forms, and receipts as required.
9. Protect all media used on the computer(s) by properly classifying, labeling, controlling, transmitting, and destroying it in accordance with security requirements.
10. Protect all hard copy produced at the highest classification level of system approval until

reviewed for proper classification and control.

11. Notify the Information System Security Officer when access to the computer(s) is no longer needed (e.g., transfer, termination, leave of absence, or for any period of extended non-use).
12. Choose a password in compliance with DOJ password policies and change that password as required by the password policies. In addition, use a different password than is used on other DOJ systems.
13. Protect the password as classified information at the level of classification authorized for the computer(s).
14. Ensure compliance with software and copyright laws.
15. Obtain permission from the Information System Security Officer, before changing any of configurations and settings of the operating system and security-related software.
16. Never install any software without the explicit approval of the Information System Security Officer.
17. Unless authorized by the Information System Security Officer, never add, modify, or remove hardware accessories to the computer(s).
18. Unless authorized by the Information System Security Officer, never connect any peripherals (e.g., printers) or networks to the computer(s).
19. Unless authorized by the Information System Security Officer, never access the internal components of the computer(s).
20. Make the computer(s) available at any time to the Information System Security Officer for inspection and review of audit logs.
21. Never circumvent the security mechanisms used on and by the computer(s).
22. Unless authorized by the Information System Security Officer, never test the capabilities of the security control software that is installed on the computer(s).

[redacted]

I understand that these Rules of Behavior establish standards of actions in recognition of the fact that knowledgeable users are the foundation of a successful security program, and that non-compliance to these rules will be enforced through sanctions commensurate with the level of infraction. Administrative actions due to failure to follow these Rules of Behavior may range from a verbal or written warning, removal of system access for specific period of time, reassignment to other duties, to termination, depending on the severity of the violation. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

Printed Name of User

Date

Signature

ATTACHMENT 3: HARDWARE AND SOFTWARE CONFIGURATIONS OF CLASSIFIED LAPTOP AND STANDALONE COMPUTERS

Classified Laptop Computers

- Recommended Hardware Configuration
  - A laptop computer with a currently available microprocessor.
  - 256 Mbytes of memory or more.
  - 40 Gbytes of hard disk space (or more) completely encrypted by ITSS-approved disk encryption software.
  - Floppy disk drive (Read/Write/Execute/Delete)
  - CD ROM drive (Read/Write/Execute)
  - Mouse connected through P2 port.
  - Printer connected through USB or parallel port.

- Mandatory Hardware Features
  - Wired connections between all components (e.g., laptop screen, laptop base, printer, mouse)
  - All Ethernet and modem cards are disabled.
  - Docking station port physically disabled.
  - Infrared hardware physically disabled.
  - All wireless ports physically disabled.
  - All unused ports physically disabled.
  - Boot only from hard disk to properly start the hard disk encryption/decryption software.
  - No network connectivity permitted.

- Software Configuration
  - Current DOJ-approved operating system with the ITSS-approved service pack.
  - DOJ-approved disk encryption software.
  - DOJ-approved office suite software including word processor, spreadsheet, and presentation graphics
  - DOJ-approved anti-virus software, with current virus signatures.
  - Software drivers for infrared and wireless ports must be removed or disabled.

Classified Stand-Alone Computers

- Recommended Hardware Configuration
  - A desktop computer with a currently available microprocessor.
  - 256 Mbytes of memory or more.

- 40 Gbytes of hard disk space (or more) completely encrypted by DOJ-approved disk encryption software.
- Floppy disk drive (Read/Write/Execute/Delete)
- CD ROM drive (Read/Write/Execute)
- Mouse connected through P2 port.
- Printer connected through USB or parallel port.

- Mandatory Hardware Features
  - Wired connections between all components (e.g., monitor, system unit, printer, mouse)
  - All Ethernet and modem cards are disabled.
  - Infrared hardware physically disabled.
  - All wireless ports physically disabled.
  - All unused ports physically disabled.

- Software Configuration
  - Current DOJ-approved operating system with the DOJ-approved service pack.
  - DOJ-approved disk encryption software.
  - DOJ-approved office suite software including word processor, spreadsheet, and presentation graphics
  - DOJ-approved anti-virus software, with current virus signatures.
  - Software drivers for infrared and wireless ports must be removed or disabled.

Computers with Removable Hard Drives

- Recommended Hardware Configuration
  - An Intel-based laptop computer with a Pentium IV microprocessor.
  - 256 Mbytes of memory or more.
  - Removable hard disk with 40 Gbytes of hard disk space (or more) completely encrypted by the ITSS-approved encryption software.
  - Removable hard disk receptacle with a key lock.
  - Floppy disk drive (Read/Write/Execute/Delete)
  - CD ROM drive (Read/Write/Execute)
  - Mouse connected through P2 port.
  - Printer connected through USB or parallel port.

- Mandatory Hardware Features
  - Wired connections between all components (e.g., monitor, system unit, printer, mouse)
  - All Ethernet and modem cards are disabled.
  - Infrared hardware physically disabled.

- All wireless ports physically disabled.
- All unused ports physically disabled.

- Software Configuration
  - Current DOJ-approved operating system with the DOJ-approved service pack.
  - DOJ-approved disk encryption software.
  - DOJ-approved office suite software including word processor, spreadsheet, and presentation graphics
  - DOJ-approved anti-virus software, with current virus signatures.
  - Software drivers for infrared and wireless ports must be removed or disabled.

ATTACHMENT 4: LIST OF ACRONYMS

AO	Authorizing Official
C&A	Certification and Accreditation
CA	Certification Agent
CIO	Chief Information Officer
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DOJ	Department of Justice
DOJ CERT	DOJ Computer Emergency Response Team
DSO	Department Security Officer
FIPS	Federal Information Processing Standard
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITSS	Information Technology and Security Staff
NIACAP	National Information Assurance Certification and Accreditation Process
PC	Personal Computer
SA	System Administrator
SEPS	Security and Emergency Planning Staff
SPM	Security Program Manager
ST&E	Security Test and Evaluation

ATTACHMENT 5: SAMPLE CLASSIFIED COMPUTER USAGE LOG

Date	User/Administrator Name	Function (e.g., Word Processing, Printing, Administration)	Document Name	Time Started	Time Stopped

ATTACHMENT 6: SAMPLE CLASSIFIED COMPUTER MAINTENANCE LOG

Date	Administrator Name	Action Performed	Time Started	Time Stopped

ATTACHMENT 7: CLASSIFIED LAPTOP AND STANDALONE COMPUTER TECHNICAL CHECKLIST

☐ 1. Determine if a laptop or stand-alone (desktop) computer is more appropriate:
   a. Is a GSA-approved safe available for storage of a laptop computer or removable hard disk?
   b. Is the facility where the computer will be used approved for the open storage of classified material?

If the answer to a is "yes", a laptop computer or computer with removable hard disk is appropriate.
If the answer to b is "yes", a stand-alone computer may be used for classified processing.
If the answer to both questions is "no", classified processing cannot be performed until a safe is acquired or the facility is approved for open storage.

☐ 2. Appoint an Information System Security Officer (ISSO) and System Administrator (SA) for the classified computer. Provide the name, address, telephone number, and e-mail address of the ISSO and SA to ITSS.

☐ 3. Acquire the computer that is to be used for classified processing. Inspect the computer for completeness and verify that no tampering is evident before proceeding further. (If tampering is evident, do not use the computer for classified processing and seek guidance on appropriate steps from the Security Program Manager.)

☐ 4. The ISSO will establish a Usage Log and Maintenance Log for the computer.

☐ 5. The ISSO will attach security classification stickers. (From this point on, the computer must be treated as a classified item.)

☐ 6. The SA will configure the hardware and software:

   a. Typically, new computers will be delivered with the operating system and certain applications already installed.

   b. Verify that the computers comply with the requirement in Attachment 3 of the Classified Laptop and Stand-Alone Computers Security Policy. In particular, ensure that there are no wireless (RF or Infrared) ports active and; if necessary, disable any such ports that are found. Disable any internal modems.

c. Obtain a copy of the ITSS-approved disk encryption software from the JCON help desk.

d. If possible, prior to the installation of the disk encryption software, make a complete backup of the hard disk to support restoration of the software in the event that the disk encryption software installation does not successfully complete.

e. Install and configure the disk encryption software software.

f. Install any additional ISSO-approved application software.

g. Record on the system maintenance log that the operating system, disk encryption software software, and application software were successfully installed.

h. Disable any unneeded hardware interfaces (e.g., serial ports) and record this appropriately on the system maintenance log.

☐ 7. The ISSO will report the following about the newly-configured classified computer to the ITSS:

- Computer Model and Serial Number
- Classification Level (e.g., Top Secret)
- Date Placed In Service

☐ 8. The ISSM will arrange for an initial independent verification of the configuration and logs of the classified computer.

☐ 9. The ISSM will work with the ISSO to schedule reviews of the configurations and logs of each classified computer.

U.S. Department of Justice

Washington, D.C. 20530

JUN 21 2005

MEMORANDUM FOR GLENN A. FINE
INSPECTOR GENERAL

FROM: Vance E. Hitch
Chief Information Officer

SUBJECT: Response to DRAFT Inspector General Report on Processing Classified Information on Portable Computers in the Department of Justice

We have reviewed your draft report on the processing of classified information on portable computers in the Department and we have several comments to offer.

The Department of Justice *Security Program Operating Manual* (SPOM), November 3, 2004 contains a number of requirements that specifically apply to classified laptop and standalone computers, in addition to those requirements stated in IT Security Standard 1.6, *Classified Laptop and Standalone Computers*. Where applicable in our response, reference will be made to the appropriate section of the SPOM.

Finding #1 Standard1.6 Has Inappropriate References and is Incomplete

OIG Recommendation: Remove any references to statute, policy, or procedures that are not applicable to processing classified information.

OCIO Response: We concur. The next release of the Standard 1.6 will remove references that are not applicable to classified information. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Address systems in accordance with policy from the Committee on National Security Systems for Classified National Security Information independently from the Director of Central Intelligence Directives for Sensitive Compartmented Information.

OCIO Response: We concur. The contents of Standard 1.6 are consistent with the best practices embodied in documentation published by the Committee on National Security Systems for Classified National Security Information and the Director of Central Intelligence Directives for Sensitive Compartmented Information (SCI). ITSS will ensure that the revised version of Standard 1.6 clearly indicates which requirements are applicable only to non-SCI computers and which requirements are applicable only to SCI computers. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Indicate what policy applies when classified portable computers are allowed to be connected to classified networks.

OCIO Response: We concur. Standard 1.6 was not intended to apply when classified portable computers are allowed to be connected to classified networks. Such computers would be subject to the requirements contained in the DOJ Security Program Operating Manual (SPOM) and the other DOJ IT Security Standards. An appropriate statement that identifies the relevant policies for classified portable computers when those computers are allowed to be connected to classified networks will be added to Standard 1.6. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Refer to Attachment 2 (Security Acknowledgment Statement for System Administrators) in the body of the policy and delineate the process for reviews of the security configuration by independent testers and validation of the system security by certification agents.

OCIO Response: We concur. The next release of Standard 1.6 will include an appropriate reference in the body of the policy and will delineate the process for reviews of the security configuration by independent testers and validation of the system security by certification agents. The standard will also refer to the requirements for independent testing that are contained in the ITS Standard 2.6. Standard 1.6 is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Refer to Attachment 5 (Sample Classified Computer Usage Log) in the body of the policy and provide written instructions for the preparation and retention of the log.

OCIO Response: We concur. ITSS will determine the most appropriate way to reference Attachment 5 in the body of the policy. This reference will require use of the log and will allow the Authorizing Official to accept the risk for not using the log after a risk-based decision. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

Finding # 2 - Increasing Efficiency When Processing Classified Information on Portable Computers

OIG Recommendation: Consider the use of removable hard drives for processing both classified and unclassified information on the same portable computer by using two separate removable hard drives. This would require that the hard drive become the classifiable device instead of the portable computer and that appropriate security safeguards be developed.

OCIO Response: We concur. This has been a proven process in the past. This scenario is explicitly supported by section 8-304 in the SPOM. The next release of Standard 1.6 will support this concept of operations. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Document the process that gives DOJ components the flexibility to incorporate safeguards through new type accreditations to protect classified computers from unauthorized access.

OCIO Response: We concur. ITSS will update Standard 1.6 to encourage components to utilize a type accreditation for non-networked classified computers. ITSS will add a section to Standard 1.6 to address accreditation requirements and endorse the concept of type accreditation for non-networked classified computers. Reference will be made to the JMD type accreditation package and that components have the flexibility to incorporate appropriate additional safeguards to protect classified computers from unauthorized access. Standard 1.6 is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Adopt the encryption standard specified by the Committee on National Security Systems.

OCIO Response: We concur. The Committee on National Security Systems (CNSS) requires the use of Type I encryption to protect the transmission of classified information over public data lines and other non-secure channels. ITSS will contact the National Security Agency (NSA) during July 2005 to determine the current status of initiatives to develop encryption standards for data stored on classified computers. To the extent that such standards are available from the CNSS and NSA, Standard 1.6 will be revised to reference these encryption standards. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Consider enhancing security by writing policy to limit classified data on a hard drive to what is necessary to accomplish the mission.

OCIO Response: We concur. The next update of Standard 1.6 will specifically address this recommendation. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

OIG Recommendation: Consider enhancing security by programming the computer to send a message to the system administrator if a computer with a classified hard drive is connected to the Internet.

OCIO Response: We concur. The OCIO is working with other agencies and industry to find ways to enhance security across the DOJ. This would include mechanisms to securely notify the system administrator if a computer with a classified hard drive was connected to the Internet. The ITSS will send a request to the Department of Homeland Security Science and Technology Directorate by July 30, 2005 requesting that the DHS issue guidance about such capabilities.

OIG Recommendation: Consider enhancing security by installing an electronic device on portable computers to track the equipment in the event it is lost or stolen.

OCIO Response: We concur. At this time, it appears that such tracking mechanisms require a substantial facilities infrastructure that could not be justified to track a limited number of classified computers. In addition, any such device that includes a transmitter is not permitted in Sensitive Compartmented Information Facilities (SCIFs). ITSS will send a request to the Department of Homeland Security Science and Technology Directorate by July 30, 2005 requesting that the DHS issue guidance about such tracking mechanisms.

OIG Recommendation: Create a new label for portable computers that indicates the computer may contain classified information, but is also cleared to process unclassified information.

OCIO Response: We concur. Section 8-304 of the November 2004 version of the DOJ Security Program Operating Manual (SPOM) addresses the labeling of computers that use removable drives to switch between classified operations and unclassified operations. The SPOM requires the use of different banners to be displayed on computer screens for unclassified and classified processing. The next version of Standard 1.6 will reference this section of the SPOM. The standard is currently being revised and will be released for component review by July 30, 2005. The revised standard will be finalized by September 30, 2005.

Thank you for the opportunity to review the draft report, if you have any questions or require additional information, please contact Kevin Deeley on (202) 353-2421 or via email at kevin.deeley@usdoj.gov.

APPENDIX V

OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION, ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

Recommendation Number:

1. **Resolved.** The Office of the Chief Information Officer (OCIO) agreed with our recommendation. The OCIO will revise Standard 1.6 to remove any reference to statutes, policies, or procedures that is not applicable to classified information processing. The OCIO expects that the next revision of Standard 1.6 will be finalized by the end of September 2005. To close this recommendation, the OCIO should provide us a draft copy of the of the Standard 1.6 revision.

2. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to address systems according to policy from the Committee on National Security Systems (CNSS) for Classified National Security Information independently from the Director of Central Intelligence Directives for Sensitive Compartmented Information (SCI). The OCIO stated that the Standard 1.6 revision will indicate the requirements applicable to both non-SCI and SCI computers. To close this recommendation, the OCIO should provide us a draft copy of the of the Standard 1.6 revision.

3. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to indicate what policies apply when classified portable computers are allowed to be connected to classified networks. The OCIO stated that it will add a statement identifying relevant policies to connect classified portable computers to classified networks to the revised Standard 1.6. To close this recommendation, the OCIO should provide us a draft copy of the of the Standard 1.6 revision.

4. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to both reference Attachment 2 (Security Acknowledgement Statement for System Administrators) and delineate the process used to review the security configuration by independent testers and validate system security by certification agents. To close this recommendation, the OCIO should provide us a draft copy of the of the Standard 1.6 revision.

5. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to reference Attachment 5 (Sample Classified Computer Usage Log) and provide written instructions for the preparation and retention of the log. The OCIO also stated that a reference to Attachment 5 will require use of the log and allow an Authorizing Official to accept the risk for not using the log after a risk-based decision. To close this recommendation, the OCIO should provide us a draft copy of the of the Standard 1.6 revision.

6. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to include the use of removable hard drives for processing both classified and unclassified information on the same portable computer by using two separate removable hard drives. To close this recommendation, the OCIO should provide us a draft copy of the Standard 1.6 revision.

7. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to encourage components to use an accreditation process for non-networked classified computers. To do this, the OCIO will add a section to Standard 1.6 addressing accreditation requirements and endorsing the concept of type accreditation for non-networked classified computers. Additionally, the OCIO stated that a revised Standard 1.6 will allow components the flexibility to incorporate appropriate additional safeguards to protect classified computers from unauthorized access. To close this recommendation, the OCIO should provide us a draft copy of the Standard 1.6 revision.

8. **Resolved.** The OCIO agreed with our recommendation. In July 2005, the OCIO will contact the National Security Agency (NSA) to determine the current status of initiatives developing encryption standards for data stored on classified computers. Additionally, the OCIO will revise Standard 1.6 to reference both CNSS and NSA encryption standards. To close this recommendation, the OCIO should inform us of the outcome of NSA discussions regarding standards for data stored in classified computers and provide us a draft copy of the Standard 1.6 revision.

9. **Resolved.** The OCIO agreed with our recommendation. The OCIO will revise Standard 1.6 to address limiting classified data on hard drives. To close this recommendation, the OCIO should provide us a draft copy of the Standard 1.6 revision.

10. **Resolved.** The OCIO agreed with our recommendation. In July 2005, the OCIO will send a request to the Department of Homeland Security (DHS) Science and Technology Directorate to request guidance regarding mechanisms to securely notify system administrators when classified hard drives are connected to the Internet. To close this recommendation, the OCIO should inform us of the outcome of the DHS request.

11. **Resolved.** The OCIO agreed with our recommendation. In July 2005, the OCIO will send a request to the DHS Science and Technology Directorate regarding tracking mechanisms. However, the OCIO commented that tracking mechanisms appear to require substantial infrastructure that may not be justified to track a limited number of classified computers. To close this recommendation, the OCIO should inform us of the outcome of the Department of Homeland Security concerning tracking mechanisms.

12. **Closed.** The OCIO agreed with our recommendation. The OCIO indicated that the Security Program Operating Manual (SPOM) now addresses the labeling of computers using removable drives to switch between classified and unclassified operations. Different banners will be displayed on computer screens for unclassified and classified processing.