



Department of Defense INSTRUCTION

NUMBER 8552.01
October 23, 2006

ASD(NII)/DoD CIO

SUBJECT: Use of Mobile Code Technologies in DoD Information Systems

- References:
- (a) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
 - (b) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
 - (c) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
 - (d) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," November 7, 2000 (hereby canceled)
 - (e) through (k), see Enclosure 1

1. PURPOSE

This Instruction:

1.1. Establishes and implements policy on using mobile code in DoD information systems according to References (a) and (b) and the authority in Reference (c).

1.2. Cancels Reference (d) and Deputy Assistant Secretary of Defense for Networks and Information Integration Memorandum (Reference (e)).

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.1.2. All DoD-owned or DoD-controlled information systems used to process, transmit, store, or display DoD information. This includes mobile devices (e.g., cellular phones, handheld devices) capable of executing mobile code.

2.2. This Instruction does not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information and special access programs for intelligence as directed by Executive Order 12333 (Reference (f)) or other laws and regulations.

2.3. Mobile code that originates from and travels exclusively within a single enclave boundary is exempt from the requirements of this Instruction. However, if an enclave consists of geographically dispersed computing environments that are connected by the Non-Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), Internet, or a public network, the requirements of this Instruction shall be met.

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Each mobile code technology to be used in DoD information systems shall undergo a risk assessment, be assigned to a risk category, and have its use regulated based on its potential to cause damage to DoD operations and interests if used maliciously. The characteristics of the mobile code risk categories and the usage restrictions are detailed in Enclosure 3.

4.2. Risk category assignments and use restrictions for commonly used mobile code technologies shall be documented in a Mobile Code Risk Category Assignments List published and updated at least annually by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO).

4.3. When required to conduct official business, all mobile code technologies that are permitted to be used in DoD information systems under this Instruction shall be allowed to pass through DoD enclave boundary protection mechanisms.

4.4. All DoD-owned and DoD-controlled servers shall be monitored to detect the presence of prohibited mobile code. Any discovered prohibited mobile code shall be removed.

4.5. All mobile code-enabled software residing on workstations and servers shall be configured compliant with the "Configuration Guidance for Client Workstations and Applications to Implement the DoD Policy on the Use of Mobile Code" (hereafter referred to as

“DoD mobile code policy implementation guidance”) issued on the DoD Information Assurance Support Environment (IASE) Web site (Reference (g)).

4.6. Mobile code-enabled software residing on workstations and servers shall be monitored to ensure its configuration is compliant with Reference (g). Identified misconfigurations shall be corrected immediately.

5. RESPONSIBILITIES

5.1. The ASD(NII)/DoD CIO shall:

5.1.1. Monitor the implementation of this Instruction and ensure all mobile code technologies used within the Department of Defense are assigned to a risk category.

5.1.2. Publish updates to the Mobile Code Risk Category Assignments List, as required.

5.1.3. Make trust decisions regarding non-DoD code-signing certificates used by Web sites that are trusted sources throughout the Department of Defense to sign their Category 1A or Category 2 mobile code. (See section E3.7.4.)

5.1.4. Ensure the currency of Reference (g) and the “Mobile Code Developer’s Guide” (hereafter referred to as “mobile code developer’s guidance”) issued on the IASE Web site (Reference (h)).

5.2. The Director, Defense Information Systems Agency (DISA), under the authority, direction, and control of the ASD(NII)/DoD CIO, shall:

5.2.1. Support the development of References (g) and (h) and ensure the DoD Security Technical Implementation Guides issued on the IASE Web site (Reference (i)) appropriately incorporate relevant guidance from References (g) and (h).

5.2.2. Manage the periodic review and update of the Mobile Code Risk Category Assignments List; forward updates to the Office of the ASD(NII)/DoD CIO (OASD(NII)/DoD CIO) for publication.

5.2.3. In coordination with the DoD Components, prioritize mobile code technologies nominated to undergo a security assessment and forward the nominations to the Director, National Security Agency (NSA), for assessment.

5.2.4. Review the risk assessments provided by NSA, and in consultation with OASD(NII)/DoD CIO and the DoD Components as appropriate, assign each mobile code technology to a risk category.

5.2.5. In coordination with the Director, NSA, facilitate the use of DoD code-signing certificates for digital signature of mobile code.

5.3. The Director, NSA, under the authority, direction, and control of the ASD(NII)/DoD CIO for network operations and IA matters according to Reference (c), shall:

5.3.1. Conduct risk assessments of mobile code technologies and recommend the assignment of mobile code technologies to specific risk categories.

5.3.2. Provide technical advice and assistance in the development of countermeasures to identified risks associated with specific mobile code technology implementations.

5.3.3. Support the development of DoD mobile code policy implementation and developer's guidance (References (g) and (h)).

5.3.4. In coordination with the Director, DISA, facilitate the use of DoD code-signing certificates for digital signature of mobile code.

5.4. The Heads of the DoD Components shall:

5.4.1. Configure workstation and server mobile code-enabled software to be compliant with Reference (g).

5.4.2. Ensure all workstation and server mobile code-enabled software configurations are monitored to identify and immediately correct misconfigurations.

5.4.3. Ensure all Component development, acquisition, upgrade, or modification efforts for DoD information systems (including outsourced IT-based processes), as a minimum, comply with Reference (h).

5.4.4. Ensure all mobile code that resides on Component servers complies with the usage restrictions provided in Enclosure 3.

5.4.5. Use additional risk mitigation tools and strategies to reduce the risk of using mobile code in DoD information systems as they become available.

5.4.6. Ensure that mobile code technologies are included as part of the information assurance (IA) awareness program to alert and train personnel, including both users and IA technicians, on the risks and appropriate use of mobile code technologies and the need to maintain secure configurations of all mobile code-enabled software.

5.4.7. Nominate to the Director, DISA, mobile code technologies to undergo a risk assessment and assignment or reassignment to specific risk categories.

5.4.8. Identify and designate as trusted those non-DoD code-signing certificates used to sign Category 1A or Category 2 mobile code residing on Web sites that are trusted sources within the Component. (See section E3.7.4.)

5.4.9. Ensure the Component's enclave boundary protection mechanisms are configured to allow all permitted mobile code technologies to pass through the Component's enclave boundaries when required to conduct official business.

5.4.10. Ensure all Component-owned and Component-controlled servers are monitored to detect the presence of mobile code that is prohibited by this Instruction to the extent possible, and that any discovered prohibited mobile code is removed from the Component's servers.

5.4.11. Ensure any prohibited mobile code discovered on DoD servers is reported to the Commander, Joint Task Force – Global Network Operations, in accordance with DoD Instruction O-8532.2 (Reference (j)).

5.4.12. Implement a process within their Components for issuing and managing DoD code-signing certificates. The process shall include designating staff authorized to obtain code-signing certificates and sign mobile code that will reside on DoD servers on the Component's behalf. The process shall be in accordance with DoD Instruction 8520.2 (Reference (k)).

5.5. The Commander, U.S. Strategic Command, through the Chairman of the Joint Chiefs of Staff, shall, in addition to performing the responsibilities in paragraph 5.4.:

5.5.1. Ensure that all DoD servers are monitored to detect the presence of prohibited mobile code.

5.5.2. Coordinate with the DoD Components to ensure that any discovered prohibited mobile code is expeditiously removed from DoD servers.

5.5.3. Coordinate with the DoD Components to ensure that all permitted mobile code technologies are allowed to pass through DoD enclave boundary protection mechanisms when required to conduct official business.

5.5.4. Identify and assess commercial off-the-shelf tools that may be useful in implementing this Instruction in a defense-in-depth approach, including:

5.5.4.1. Enclave boundary protection tools capable of detecting and blocking prohibited types of mobile code at the enclave boundary.

5.5.4.2. Runtime code monitoring and protection products that reside on client workstations and hosts that are capable of intercepting an application's attempts to perform suspicious activities (e.g., modifying the Windows Registry) based on a customizable security policy.

5.5.4.3. Software inventory tools capable of monitoring servers and workstations and detecting the presence of prohibited types of mobile code.

5.5.4.4. IA vulnerability and exposure remediation products to automate the process of securely configuring mobile code-enabled software, particularly tools capable of scanning and

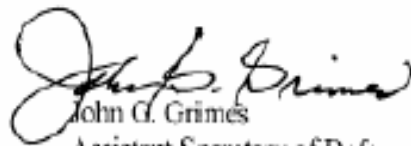
identifying software misconfigurations and vulnerabilities and automatically remediating the misconfigurations.

6. PROCEDURES

Mobile code risk category characteristics and usage restrictions are detailed in Enclosure 3.

7. EFFECTIVE DATE

This Instruction is effective immediately.



John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures – 3

- E1. References, continued
- E2. Definitions
- E3. Mobile Code Risk Categories Characteristics and Usage Restrictions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Deputy Assistant Secretary of Defense for Networks and Information Integration Memorandum, “Mobile Code Technologies Risk Category Assignments and Use Restrictions,” January 20, 2006 (hereby canceled)
- (f) Executive Order 12333, “United States Intelligence Activities,” December 4, 1981
- (g) DoD Information Assurance Support Environment Web site, “Configuration Guidance for Client Workstations and Applications to Implement the DoD Policy on the Use of Mobile Code,” <https://iase.disa.mil/mcp/index.html>
- (h) DoD Information Assurance Support Environment Web site, “Mobile Code Developer’s Guide,” <https://iase.disa.mil/mcp/index.html>
- (i) DoD Information Assurance Support Environment Web site, DoD Security Technical Implementation Guides, <https://iase.disa.mil/stigs/stig/index.html>
- (j) DoD Instruction O-8530.2, “Support to Computer Network Defense (CND),” March 9, 2001¹
- (k) DoD Instruction 8520.2, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” April 1, 2004

¹ Available from the office of the ASD(NII)/DoD CIO.

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Assured Channel. A network communication link that is protected by a security protocol providing authentication and data integrity, and employs cryptographic technologies approved by the U.S. Government (USG) whenever cryptographic means are used. Examples of protocols and mechanisms that may be used to provide authentication and data integrity protection for an assured channel include Internet Protocol Security (IPSec), Secure Sockets Layer (SSL), Transport Layer Security (TLS), digital code signing using a trusted code-signing certificate, and other systems using NSA-approved high assurance guards with link encryption methodology.

E2.2. Code-Signing Certificate. A Public Key Infrastructure (PKI) certificate whose associated private key can be used for digitally signing code. Such a certificate has a specially assigned attribute, referred to as the code-signing Object Identifier, set to Enabled. (Although this Instruction refers to signing mobile code using a code-signing certificate, operationally it is the certificate's associated private key that is used to sign mobile code.)

E2.2.1. DoD Code-Signing Certificate. A code-signing certificate issued by a certificate authority that is owned or operated by the Department of Defense.

E2.2.2. External Certificate Authority (ECA) Code-Signing Certificate. A code-signing certificate issued by an approved ECA. ECA certificates are intended to be used by organizations (e.g., companies, non-profit organizations, universities) that do business with the Department of Defense to sign mobile code that resides on their Web sites.

E2.2.3. USG Code-Signing Certificate. A code-signing certificate issued by a certificate authority owned or operated by a non-DoD USG organization (e.g., the Department of Energy, the Department of Homeland Security).

E2.2.4. Commercial Code-Signing Certificate. A code-signing certificate issued by a commercial certificate authority.

E2.2.5. Non-DoD Code-Signing Certificate. A commercial code-signing certificate, an ECA code-signing certificate, or a USG code-signing certificate.

E2.3. Constrained Execution Environment. A runtime environment that constrains mobile code to prevent its access to local system and network resources including the local file system, operating system settings, and parameters (e.g., Microsoft Windows Registry), and its ability to establish network connections other than to the mobile code's originating server. Examples of constrained execution environments include Java Runtime Environment sandbox, .NET Common Language Runtime, and a browser's JavaScript sandbox.

E2.4. DoD Information System. For the purposes of this Instruction, a set of information resources organized for the collection, storage, processing, maintenance, use, sharing,

dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes, and platform IT interconnections.

E2.5. Emerging Mobile Code Technologies. All mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and been assigned to a risk category.

E2.6. Enclave. For the purposes of this Instruction, a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (Enclaves are defined by their IA Certification and Accreditation boundary.)

E2.7. Enclave Boundary. For the purposes of this Instruction, the point at which an enclave's internal network service layer connects to an external network's service layer.

E2.8. Enclave Boundary Protection Mechanism. Hardware and/or software products that protect enclave boundaries by filtering network connections, filtering network protocols, controlling access to network ports, controlling information transfers, and/or controlling the flow of mobile code. Examples include firewalls, proxy filters, and gateway mobile code content filters.

E2.9. Malicious Mobile Code. For the purposes of this Instruction, mobile code software designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources.

E2.10. Mediated Access. Access to system resources subject to the control and approval of a runtime-enforced security policy, either during execution or at the beginning of execution. A runtime-enforced security policy provides controlled access to system resources via an intermediary such as an interpreter, virtual machine, or security manager.

E2.11. Mobile Agent. A type of mobile code that is autonomous, intelligent, and can migrate from machine to machine throughout a heterogeneous network, deciding when and where to migrate, and maintaining its state. Mobile agents initiate their own execution and migration from one platform to another without any user interaction. A supporting mobile agent platform typically resides on a machine to receive migrating mobile agents at runtime. Mobile agents may be implemented as scripts, intermediate languages (e.g., Java), or binary executables (e.g., C++).

E2.12. Mobile Agent Technologies. Software technologies that provide the mechanisms for the production and use of mobile agents (e.g., Tcl, Aglets).

E2.13. Mobile Code. For the purposes of this Instruction, software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

E2.14. Mobile Code Technologies. Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java Virtual Machine, Java compiler, .NET Common Language Runtime, Windows Scripting Host, HTML Application Host).

E2.15. Mobile Code-Enabled Software. Software that is capable of executing one or more types of mobile code. Examples include operating systems (i.e., Microsoft Windows), office applications (e.g., Microsoft Office, Corel Office), browsers (e.g., Internet Explorer, Netscape, Mozilla, Firefox), email clients (e.g., Outlook, Outlook Express, Mozilla, Netscape, Thunderbird, Eudora), mobile code runtime environments (e.g., Sun Java Virtual Machine, .NET Common Language Runtime, Adobe Reader, Macromedia Shockwave Director, Macromedia Flash, Postscript readers), and mobile agent systems.

E2.16. Permitted Mobile Code. Those types of mobile code that are allowed to be used in accordance with this Instruction when the associated usage requirements are implemented. Permitted mobile code includes signed Category 1A mobile code, unsigned Category 2 mobile code that executes in a constrained execution environment, Category 2 mobile code obtained from a trusted source over an assured channel, Category 3 mobile code, and mobile code that downloads via email that does not execute automatically when the user opens the email body or attachment.

E2.17. Prohibited Mobile Code. Those types of mobile code that are prohibited from being used in DoD information systems in accordance with this Instruction. Prohibited mobile code includes all Category 1X mobile code, unsigned Category 1A mobile code, Category 2 mobile code that violates this Instruction's usage requirements, all Emerging Technologies mobile code, and all mobile code that downloads via an email body or email attachment that executes automatically when the user opens the email body or attachment.

E2.18. Remediation of Software Misconfigurations. Correction of software misconfigurations.

E2.19. Trusted Code-Signing Certificates. DoD code-signing certificates, ECA code-signing certificates, and commercial and USG code-signing certificates that have been designated as trusted by the DoD CIO or the responsible Component CIO.

E2.20. Trusted Server. A server that hosts a trusted Web site.

E2.21. Trusted Source. A software and/or information source that is adjudged to provide reliable software code and/or information and whose identity can be verified by authentication. Examples of mechanisms that may be used to validate the identity of a trusted source include applying a digital signature over the mobile code itself using a trusted code-signing certificate,

and authenticating the source of the transfer by public key certificate (e.g., SSL server certificate from an SSL Web server).

E2.22. Trusted Web Site. A Web site (typically identified by a domain name) that has been designated as a trusted source within a Component for the purposes of this Instruction. A Web site may be hosted on one or more servers. Servers that host trusted Web sites are sometimes referred to as trusted servers. DoD typically requires the use of trusted Web sites to conduct official business.

E2.23. Unmediated Access. Direct use of system resources, not subject to any approval or control by a runtime-enforced security policy beyond that imposed on conventional user applications.

E3. ENCLOSURE 3

MOBILE CODE RISK CATEGORIES CHARACTERISTICS AND USAGE RESTRICTIONS

E3.1. GENERAL

This Enclosure defines the DoD mobile code risk categories, describes their characteristics, and establishes restrictions for the acquisition (to include development) and use of mobile code technologies assigned to each risk category. It also establishes restrictions on the use of mobile code in email and emerging mobile code technologies. For the purposes of this Instruction, the SIPRNet and NIPRNet do not meet the definition of an enclave.

E3.1.1. The primary means of implementing this Instruction is by securely configuring all mobile code-enabled software residing on workstations and servers. In addition, as part of a defense-in-depth approach, prohibited types of mobile code shall be blocked at the enclave boundary to the extent possible.

E3.1.2. To the extent possible, all DoD-owned and DoD-controlled servers shall be monitored to detect the presence of prohibited types of mobile code; all identified prohibited mobile code shall be removed from the servers.

E3.1.3. DoD-owned and DoD-controlled servers shall be trusted sources by default.

E3.1.4. DoD code-signing certificates shall be designated as trusted by default by all the Components.

E3.1.5. DoD contractual arrangements should require outsourced IT-based processes that include servers to meet this Instruction's requirements, to the extent possible. Outsourced IT-based processes should obtain ECA code-signing certificates and use them to sign any Category 1A mobile code that resides on their servers. Similarly, when an outsourced IT-based process uses code signing to meet Category 2 usage restrictions, the outsourced IT-based process should use ECA code-signing certificates to sign the Category 2 mobile code that resides on their servers.

E3.2. CATEGORY 1 MOBILE CODE

E3.2.1. Category 1 mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server, and remote system services and resources. Category 1 mobile code technologies have known security vulnerabilities with few or no countermeasures once they begin executing. Execution of Category 1 mobile code typically requires an all-or-none decision: either execute with full access to all system resources or do not execute at all.

E3.2.2. Category 1 mobile code technologies pose a significant threat to DoD information systems; however, in some cases the risk can be mitigated. The implementations of some mobile

code technologies differentiate between signed and unsigned mobile code and can be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. When these capabilities are present and implemented, and when the Category 1 mobile code is digitally signed with a trusted code-signing certificate, the risk is reduced. There are two subgroups of Category 1 mobile code technologies:

E3.2.2.1. Category 1A consists of those mobile code technologies that may be used when the Category 1 usage restrictions specified in this Instruction are implemented. Category 1A technologies can differentiate between signed and unsigned mobile code and can be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code.

E3.2.2.2. Category 1X consists of those mobile code technologies that are prohibited from being used in DoD information systems because they cannot implement the required Category 1 policy restrictions. Category 1X technologies cannot differentiate between signed and unsigned mobile code or cannot be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code.

E3.2.3. The use of unsigned Category 1 mobile code in DoD information systems shall be prohibited.

E3.2.3.1. To the extent possible, all unsigned Category 1 mobile code shall be blocked at the enclave boundary.

E3.2.3.2. To the extent possible, all DoD computer systems (e.g., servers), workstations, and applications capable of executing mobile code shall be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the enclave boundary, compliant with DoD mobile code policy implementation guidance (Reference (g)).

E3.2.4. If a Category 1 mobile code technology (or its implementation) cannot differentiate between signed and unsigned Category 1 mobile code, or cannot be configured to block the execution of unsigned Category 1 mobile code, then use of that mobile code technology shall be prohibited. These technologies shall be assigned to Category 1X.

E3.2.4.1. To the extent possible, prohibited Category 1X mobile code technologies shall be blocked at the enclave boundary.

E3.2.4.2. To the extent possible, prohibited Category 1X mobile code technologies shall be uninstalled and/or their use disabled in all DoD computer systems, workstations, and applications.

E3.2.5. Signed Category 1A mobile code obtained from a trusted source is acceptable for use in DoD information systems provided ALL of the following conditions are met:

E3.2.5.1. The execution of unsigned Category 1A mobile code and prohibited Category 1X mobile code shall be disabled as required in sections E3.2.3 and E3.2.4.

E3.2.5.2. The mobile code was signed with a code-signing certificate that has been designated as trusted by the recipient's Component. (See section E3.7. for code-signing certificate requirements.)

E3.2.5.3. The mobile code's digital signature is properly validated by the client runtime environment prior to the execution of the mobile code.

E3.2.5.4. To the extent possible, Web browsers and other mobile code-enabled products are configured to prompt the user prior to the execution of signed Category 1A mobile code, compliant with DoD mobile code policy implementation guidance (Reference (g)).

E3.2.6. When the usage restrictions in section E3.2.5. can be implemented for a Category 1 mobile code technology, the technology shall be assigned to Category 1A.

E3.2.7. All Category 1A mobile code that resides on DoD-owned or DoD-controlled servers shall be signed with a DoD code-signing certificate prior to being installed on the servers. If a DoD code-signing certificate cannot be used due to interoperability issues (e.g., client runtime environments cannot properly validate mobile code signed with a DoD code-signing certificate), the DoD CIO or the responsible Component CIO may approve the use of an alternate non-DoD code-signing certificate to sign the mobile code. (See section E3.7. for code-signing certificate requirements.)

E3.2.8. To enable DoD users to use non-DoD Web sites that are trusted sources and that use Category 1A mobile code signed with non-DoD code-signing certificates, the DoD CIO or the responsible Component CIO may designate as trusted the specific non-DoD code-signing certificates used by those trusted sources' Web sites. Similarly, when a DoD server uses Category 1A mobile code signed with non-DoD code-signing certificates, the DoD CIO or the responsible Component CIO may designate as trusted those specific non-DoD code-signing certificates.

E3.3. CATEGORY 2 MOBILE CODE

E3.3.1. Category 2 mobile code technologies have full functionality, allowing mediated or controlled access to workstation, server, and remote system services and resources. Category 2 mobile code technologies may have known security vulnerabilities but also have known fine-grained, periodic, or continuous countermeasures or safeguards.

E3.3.2. Category 2 mobile code technologies can pose a moderate threat to DoD information systems. The use of Category 2 mobile code technologies, when combined with prudent countermeasures against malicious use, can afford benefits that outweigh their risks.

E3.3.3. Unsigned Category 2 mobile code that executes in a constrained execution environment without access to local system and network resources (e.g., file system, Windows

Registry, network connections other than to its originating server) may be freely used in DoD information systems.

E3.3.4. Category 2 mobile code that does not execute in a constrained execution environment may be used in DoD information systems if the mobile code is obtained from a trusted source over an assured channel using at least one of the following measures:

E3.3.4.1. Code Signing

E3.3.4.1.1. The mobile code was digitally signed with a code-signing certificate that has been designated as trusted by the recipient's Component. (See section E3.7. for code-signing certificate requirements.)

E3.3.4.1.2. The mobile code's digital signature is properly validated by the client runtime environment prior to the execution of the mobile code.

E3.3.4.2. SSL Connection. The mobile code was downloaded over an SSL connection from a trusted SSL Web server using a DoD or trusted commercial SSL server certificate.

E3.3.4.3. TLS Connection. The mobile code was downloaded over a TLS connection from a trusted TLS Web server using a DoD or trusted commercial TLS server certificate.

E3.3.4.4. IPSec Combined with Mutual Authentication. The mobile code was downloaded from a trusted Web server over an encrypted IPSec connection that establishes mutual authentication using a DoD or trusted commercial certificate.

E3.3.5. To the extent possible, Web browsers and other mobile code-enabled products shall be configured to prompt the user prior to the execution of Category 2 mobile code, compliant with DoD mobile code policy implementation guidance (Reference (g)). Where feasible, protections against malicious Category 2 mobile code technologies shall be employed at DoD information system end-user systems and at enclave boundaries.

E3.3.6. If code signing is used to meet the requirement for a trusted source over an assured channel for mobile code that will reside on a DoD-owned or DoD-controlled server, the mobile code shall be signed with a DoD code-signing certificate prior to being installed on the server. If a DoD code-signing certificate cannot be used due to interoperability issues (e.g., client runtime environments cannot properly validate mobile code signed with a DoD code-signing certificate), then the DoD CIO or the responsible Component CIO may approve the use of an alternate non-DoD code-signing certificate to sign the mobile code. (See section E3.7. for code-signing certificate requirements.)

E3.3.7. To enable DoD users to use non-DoD Web sites that are trusted sources and that use Category 2 mobile code signed with non-DoD code-signing certificates, the DoD CIO or the responsible Component CIO may designate as trusted the specific non-DoD code-signing certificates used by those trusted sources' Web sites. Similarly, when a DoD server uses Category 2 mobile code signed with non-DoD code-signing certificates, the DoD CIO or the

responsible Component CIO may designate as trusted those specific non-DoD code-signing certificates.

E3.4. CATEGORY 3 MOBILE CODE

E3.4.1. Category 3 mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code technologies may have a history of known vulnerabilities, but also support fine-grained, periodic, or continuous security safeguards.

E3.4.2. Category 3 mobile code technologies pose limited risk to DoD information systems. When combined with vigilance comparable to that required to keep any software system configured to resist known exploits, the use of Category 3 mobile code affords benefits that outweigh the risks.

E3.4.3. Category 3 mobile code technologies may be freely used without restrictions in DoD information systems.

E3.5. EMERGING MOBILE CODE TECHNOLOGIES

E3.5.1. Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and been assigned to one of the three risk categories described above.

E3.5.2. Because of the uncertain risk, the use of emerging mobile code technologies in DoD information systems shall be prohibited.

E3.5.2.1. To the extent possible, emerging mobile code technologies shall be blocked at the enclave boundary.

E3.5.2.2. To the extent possible, emerging mobile code technologies shall be uninstalled and/or their use disabled in all DoD computer systems, workstations, and applications.

E3.5.3. If an emerging mobile code technology is planned for use in a DoD application, the sponsoring DoD Component shall nominate the mobile code technology to undergo a risk assessment and wait for its formal assignment to a risk category prior to initial use.

E3.6. MOBILE CODE IN EMAIL

E3.6.1. Mobile code can be embedded in an email body or an email attachment and can be downloaded as part of the actual email. Alternately, mobile code residing on a remote server can be referenced from within an email body or attachment and can be automatically downloaded and executed. Some types of mobile code execute automatically as soon as the user clicks on the message subject or previews the message; others execute when the user opens an attachment

containing mobile code. Email viruses, worms, and Trojan horses typically utilize mobile code technologies; they are forms of malicious mobile code sent to users via email.

E3.6.2. Due to the significant risk of malicious mobile code downloading into user workstations via email, and the ease of rapidly spreading malicious mobile code via email, the following restrictions apply to all types of mobile code in email independent of risk category:

E3.6.2.1. To the extent possible, the automatic execution of all categories of mobile code in email bodies and attachments shall be disabled, compliant with DoD mobile code policy implementation guidance (Reference (g)).

E3.6.2.2. To the extent possible, mobile code-enabled software shall be configured to prompt the user prior to opening email attachments that may contain mobile code, compliant with Reference (g).

E3.7. CODE-SIGNING CERTIFICATE REQUIREMENTS

The code-signing certificates used to sign Category 1A and Category 2 mobile code shall meet the requirements below. (See sections E3.2. and E3.3. for Category 1A and Category 2 usage requirements.)

E3.7.1. DoD code-signing certificates (i.e., their associated private keys) shall be used to sign Category 1A mobile code that will reside on DoD-owned or DoD-controlled servers prior to its installation on the servers. When code signing is used to meet the requirements for Category 2 mobile code that will reside on DoD-owned or DoD-controlled servers, the mobile code shall be signed with DoD code-signing certificates prior to its installation on the servers. DoD code-signing certificates shall be designated as trusted by default by all Components. DoD-owned and DoD-controlled servers shall be trusted sources by default.

E3.7.2. If a DoD code-signing certificate cannot be used to sign mobile code that will reside on a DoD-owned or DoD-controlled server due to interoperability issues, the DoD CIO or the responsible Component CIO may approve the use of an alternate code-signing certificate (e.g., commercial code-signing certificate, USG code-signing certificate) to sign the mobile code.

E3.7.3. When a DoD server uses Category 1A or Category 2 mobile code signed with non-DoD code-signing certificates, the DoD CIO or the responsible Component CIO may designate as trusted those specific non-DoD code-signing certificates to enable Component users to use the DoD server.

E3.7.4. To enable DoD users to conduct official business using non-DoD Web sites that use Category 1A or Category 2 mobile code signed with non-DoD code-signing certificates, the DoD CIO and the responsible Component CIO have the authority to designate as trusted those non-DoD code-signing certificates used by trusted sources. The DoD CIO shall decide whether to trust code-signing certificates used by Web sites that are trusted sources throughout the Department of Defense. The responsible Component CIO shall decide whether to trust the code-

signing certificates used by Web sites that are trusted sources within the Component. Trust decisions shall be made using the following process:

E3.7.4.1. The DoD CIO or the responsible Component CIO shall identify non-DoD Web sites that use Category 1A or Category 2 signed mobile code that are to be trusted sources.

E3.7.4.2. For each trusted source, the responsible CIO shall identify the specific non-DoD code-signing certificates used to sign the Category 1A and Category 2 mobile code residing on the trusted source's Web site. The CIO shall then determine if the issuing certificate authority's practices warrant trusting the certificates. If the certificate authority's practices do not warrant trusting the certificates, then the code-signing certificates cannot be trusted and Category 1A and Category 2 mobile code signed with the certificates cannot be executed in DoD information systems.

E3.7.4.3. If the certificate authority's practices warrant trusting the certificates, the responsible CIO shall designate as trusted the specific non-DoD code-signing certificates that were used to sign the mobile code residing on the trusted sources' Web sites. (The CIO should NOT trust all code-signing certificates issued by the non-DoD certificate authority, only the specific certificates used by trusted sources' Web sites.)

E3.7.5. ECA code-signing certificates are intended to be used by organizations that do business with the Department of Defense to sign mobile code that resides on their Web sites. ECA code-signing certificates used to sign mobile code residing on trusted sources' Web sites shall be designated as trusted by default.

E3.7.6. Code-signing certificates that have been designated as trusted within the Component shall be pre-installed into the Component's client runtime environments (e.g., browsers, email clients, Java Runtime Environment) to facilitate the download and execution of mobile code from trusted sources. Code-signing certificates that have been designated as trusted DoD-wide shall also be pre-installed into the Component's client runtime environments.

E3.7.7. The client runtime environments (e.g., browsers, email clients, Java Runtime Environment) that download and execute mobile code shall be capable of accepting and trusting individual code-signing certificates. Client runtime environments that are only capable of basing trust decisions on the certificate authority that issued a code-signing certificate should not be used in DoD information systems.

E3.8. REQUIREMENTS FOR NEW PROCUREMENT AND DEVELOPMENT EFFORTS

E3.8.1. All program offices with new procurement and development efforts that rely on mobile code technologies shall include a mobile code risk mitigation strategy detailing the measures incorporated into the system development to curtail the risk posed by its use, in accordance with References (a) and (b). The risk mitigation strategy shall be included in the accreditation package.

E3.8.2. All DoD information system development efforts shall provide evidence of compliance with mobile code developer's guidance (Reference (h)) as part of their IA Certification and Accreditation Package. The evidence shall be associated with DoD IA Control DCMC-1, Mobile Code, as defined in Reference (b).

E3.8.3. No new DoD program may expend funds on the development or procurement of products or services that contain, use, or depend on the download and execution of Category 1 mobile code across enclave boundaries, unless that product or service uses or supports the use of signed mobile code and can implement the usage restrictions as stipulated in this Instruction. (See section E3.2.)