

Navigating Unclassified Information System Security Protections

Network Penetration Reporting and Contracting for Cloud Services





Outline

- **DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services**
 - **Safeguarding Covered Defense Information (CDI)**
 - **Identifying/Marking CDI**
 - **Adequate Security**
 - **Cyber Incident Reporting**
 - **Damage Assessment**
 - **Contracting for Cloud Services**
- **Moving Forward**
- **Resources**





Network Penetration Reporting and Contracting for Cloud Services

- **DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services, 2nd interim rule effective on December 30, 2015**
 - Revises the DFARS to implement Section 941 of NDAA for FY13 and Section 1632 of NDAA for FY15 (codified at 10 U.S.C. §§ 932 & 933)
 - Implements DoD policy and procedures for use when contracting for cloud computing services
- **Includes 3 clauses and 2 provisions:**

**Safeguarding
Covered
Defense
Information**

- (p) Section 252.204-7008, Compliance with Safeguarding Covered Defense Information
- (c) Section 252.204-7009, Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- (c) Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

**Contracting
For Cloud
Services**

- (p) Section 252.239-7009, Representation of Use of Cloud Computing
- (c) Section 252.239-7010, Cloud Computing Services





DFARS Clause 252.204-7012

	Safeguarding of Unclassified Controlled Technical Information, Nov 18, 2013 (<i>Final Rule</i>)	Safeguarding Covered Defense Information and Cyber Incident Reporting, Aug 26, 2015 (<i>Interim Rule</i>)	Safeguarding Covered Defense Information and Cyber Incident Reporting, Dec 30, 2015(<i>Interim Rule</i>)
Scope – What Information?	<ul style="list-style-type: none"> • Unclassified Controlled Technical Information 	<ul style="list-style-type: none"> • Covered Defense Information • Operationally Critical Support 	<ul style="list-style-type: none"> • Covered Defense Information • Operationally Critical Support
Adequate Security – What Minimum Protections?	<ul style="list-style-type: none"> • Selected controls in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations 	<ul style="list-style-type: none"> • NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations 	<ul style="list-style-type: none"> • NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations
When?	<ul style="list-style-type: none"> • Contract Award 	<ul style="list-style-type: none"> • Contract Award 	<ul style="list-style-type: none"> • As soon as practicable, but NLT Dec 31, 2017
When?		<p><u>Oct 8, 2015 (Deviation)</u></p> <ul style="list-style-type: none"> • Security Requirement 3.5.3, w/in 9 months of Award 	





What is Covered Defense Information?

Unclassified information that:

- Is *provided to the contractor* by or on behalf of DoD in connection with the performance of the contract; or
- Is *collected, developed, received, transmitted, used, or stored* by or on behalf of the contractor in support of the performance of the contract;

and

- Falls in any of the following categories:
 - Controlled technical information
 - Critical information (operations security)
 - Export control
 - Any other information, *marked or otherwise identified in the contract*, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information)





DFARS Procedures, Guidance, and Information

Identifying and Marking Covered Defense Information

PGI 204.73—Safeguarding Covered Defense Information and Cyber Incident Reporting

PGI 204.7303-1 General.

(b) The contracting officer shall—

(1) Ensure that covered defense information or operationally critical support, for which notification was provided in accordance with paragraph (a), is identified in the contract, task order, or delivery order;

(2) Ensure that the contract, task order, or delivery order includes the requirement (such as a contract data requirements list), as provided by the requiring activity, for the contractor to apply markings, when appropriate, on covered defense information; and

(3) Coordinate with the requiring activity for instruction regarding the disposition of covered defense information associated with the contract...





Marking Contract Data Requirements List —Block 9



Department of Defense INSTRUCTION

NUMBER 5230.24
August 23, 2012

(USIXAT&L)

SUBJECT: Distribution Statements on Technical Documents

Reference: See Enclosure 1

1. PURPOSE. This instruction:

- a. Reissues DoD Directive (DoDD) 5230.24 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDI 5134.01 (Reference (b)) and pursuant to section 133 of title 10, United States Code (U.S.C.) (Reference (c)) to establish DoD policies, assign responsibilities, and prescribe procedures for marking and managing technical documents, including research, development, engineering, test, maintenance, and logistics information, to denote the extent to which they are available for secondary distribution, release, and dissemination without additional approvals or authorizations.
- b. Establishes a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law.
- c. Facilitates implementation of DoDD 5230.25 (Reference (d)) by enabling document originators to signify to what extent technical documents must be controlled in accordance with procedures of that Directive.

2. APPLICABILITY. This instruction:

- a. Applies to:
 - (1) The OSD, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint 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 DoD (hereinafter referred to collectively as the "DoD Components").
 - (2) Newly created, revised, or previously unmarked classified and unclassified technical documents generated or managed by all DoD-funded research, development, test, and evaluation (RDTE&I) programs, which are the basis of the DoD Scientific and Technical Information

CONTRACT DATA REQUIREMENTS LIST (1 Data Item)						Form Approved OMB No. 0704-0188																																																									
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please DO NOT RETURN your form to the above address. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.																																																															
A. CONTRACT LINE ITEM NO.			B. EXHIBIT		C. CATEGORY: TDP _____ TM _____ OTHER _____																																																										
D. SYSTEM/ITEM				E. CONTRACT/PR NO.		F. CONTRACTOR																																																									
1. DATA ITEM NO.		2. TITLE OF DATA ITEM				3. SUBTITLE																																																									
4. AUTHORITY (Data Acquisition Report No.)				5. CONTRACT REFERENCE		6. REQUIRING OFFICE																																																									
7. DO 260 REF.		9. DIST STATEMENT REQUIRED		10. FREQUENCY		12. DATE OF FIRST SUBMISSION		14. DISTRIBUTION																																																							
8. APP COD				11. A/C OF DATE		13. DATE OF SUBSEQUENT SUBMISSION		a. ADDRESSEE																																																							
16. REMARKS																																																															
<table border="1"> <thead> <tr> <th colspan="2"></th> <th colspan="3">b. COPIES</th> </tr> <tr> <th colspan="2"></th> <th>Draft</th> <th>Reg</th> <th>Repro</th> </tr> </thead> <tbody> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> <tr><td colspan="2"></td><td></td><td></td><td></td></tr> </tbody> </table>											b. COPIES					Draft	Reg	Repro																																													
		b. COPIES																																																													
		Draft	Reg	Repro																																																											
								17. PRICE GROUP																																																							
								18. ESTIMATED TOTAL PRICE																																																							

Item 9. For technical data, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDD 5230.24).

No change to existing marking requirements – e.g. controlled technical information is marked in accordance with DoDI 5230.24





Network Security Controls to Safeguard Covered Defense Information

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (*effective December 30, 2015*)

- (b) Adequate security. ... To provide adequate security, the Contractor shall—**
- (1) Implement information systems security protections on all covered contractor information systems including, at a minimum—**
 - (ii) For covered contractor information systems ...**
 - (A) The security requirements in NIST SP 800-171... as soon as practical, but not later than Dec 31, 2017. The Contractor shall notify the DoD CIO... , within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award;**





Network Security Controls to Safeguard Covered Defense Information

DFARS Clause 252.204-7012 (b)(1)(ii) (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO;

- If the offeror proposes to vary from NIST SP 800-171, the Offeror shall submit to the Contracting Officer, a written explanation of -
 - Why a particular security requirement is not applicable; or
 - How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and to achieve equivalent protection

DFARS Clause 252.204-7012 (b) (2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment **based on an assessed risk or vulnerability.**





Cyber Incident Reporting

DFARS 252.204-7012 (c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

- (i) Conduct a review for evidence of compromise ...**
- (ii) Rapidly report cyber incidents to DoD ...**

What is a cyber incident?

“Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein”





What is Operationally Critical Support?

- **Supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.**
 - **Operationally Critical Support is an “activity”– not an information type – performed by the contractor.**
 - **DFARS does not require protections for contractor information systems that are used to provide operationally critical support – only the requirement for the contractor to report a cyber incident that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support.**
 - **Operationally Critical Support is not related to “Critical information (operations security)”**





Reporting a Cyber Incident

- **When DFARS Clause 252.204-7012 is included in a subcontract, subcontractors are required to rapidly report cyber incidents directly to DoD.**
 - **Subcontractors must also provide the incident report number, automatically assigned by DoD, to their prime Contractor as soon as practicable**

Where do contractors/subcontractors report?

- **DC3 is the single DoD focal point for receiving all cyber incident reporting from unclassified networks of DoD contractors**

ALL reporting will be via the Incident Collection Format (ICF) found at <http://dibnet.dod.mil>



Cyber Incident Damage Assessment Activities

DFARS 252.204-7012 (g) *Cyber incident damage assessment activities.*
If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e)* of this clause.
****(e) Media preservation and protection***

Purpose of damage assessment:

- **To understand impact of compromised information on U.S. military capability underpinned by technology**
- **Initiated after review of reported cyber incident**
- **Focused on determining impact of compromised intellectual property, not on mechanism of cyber intrusion**
- **An assessment is not possible without access to compromised material**



Safeguarding Covered Defense Information

What *IS* and is *NOT* Covered

- **Clause Prescription:** Use in *all* solicitation and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items
- **Scope of Clause:** Applies to contracts/subcontracts requiring contractors/subcontractors to safeguard *covered defense information* that resides in/transits through covered systems
- **Flowdown:** The Contractor shall include Clause in subcontracts, or similar contractual instruments, for *operationally critical support*, or for which subcontract performance will involve a *covered contractor information system*...

What <i>Is</i> Covered?	What is <i>Not</i> Covered?
The contractor's internal information system(s)	Government owned systems, systems operated on-behalf-of the government, military systems and facilities
Req't for DoD to identify/mark covered defense information	Changes to existing marking requirements for covered defense information, FOUO markings
Security controls to safeguard covered defense information	Verification, validation, certification or accreditation (e.g. RMF Authorization to Operate) of the contractor's system
Single DoD focal point for receiving all incident reports	Cyber incident reporting to any site other than <i>http://dibnet.dod.mil</i>





Contracting for Cloud Services

DFARS SUBPART 239.76 and DFARS Clause 252.239-7010

DFARS subpart 239.76, Cloud Computing:

- Implements policy developed within the DoD CIO and the **DoD Cloud Computing Security Requirements Guide (SRG)** for the acquisition of cloud computing services
- Directs use of new provision 252.239-7009, Representation of Use of Cloud Computing in solicitations for information technology services
 - Allows the offeror to represent their intention to utilize cloud computing services in performance of the contract or not.
- Directs use of **DFARS Clause 252.239-7010, Cloud Computing Services** in solicitations and contracts for information technology services
 - Provides standard contract language for the acquisition of cloud computing services, including access, security, and reporting requirements
 - Implements DoD's policies concerning Cloud Computing Services to ensure uniform application when DoD entities contract for cloud services across the DoD.

DFARS 252.239-7010(d) The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted to the Department of Defense via <http://dibnet.dod.mil/>.





Contracting for Cloud Services

What IS and is NOT Covered

- **Clause Prescription:** Use in solicitations and contracts for information technology services.
- **Scope of Clause:** Applies when using cloud computing to provide information technology services in the performance of the contract.
- **Flowdown:** The Contractor shall include the substance of the clause in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

What <i>Is</i> Covered? DoD Cloud Computing SRG applies	What is <i>Not</i> Covered? NIST SP 800-171 applies
• A cloud solution is being used to process data on the DoD's behalf	• A contractor uses his own internal cloud solution to do his processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for his internal contractor system. – Example: Contractor is developing the next generation tanker, and uses his internal cloud for the engineering design.
• DoD is contracting with Cloud Service Provider to host/process data in a cloud	
• Cloud solution is being used for processing what we (the DoD) would normally do ourselves but have decided to outsource	





What's Next in the Rule Making Process

- **The public comment period for 1st interim rule (published on Aug 26, 2015) closed on November 20, 2015.**
 - Public comments will be considered in the formation of a single final rule upon analysis of comments from the 2nd interim rule (see below).
 - DPAP, DoD CIO, and DASD(SE) are working to adjudicate comments.
- **The public comment period for 2nd interim rule (published Dec 30, 2015) closes February 29, 2016**
 - Public comments will be adjudicated and considered in the formation of a single final rule.





Resources

- **DPAP Website/DARS/DFARS and PGI**
(<http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>)
 - DFARS Subpart 204.73 and PGI 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
 - SUBPART 239.76 and PGI 239.76 – Cloud Computing
 - 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
 - 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
 - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
 - 252.239-7009 Representation of Use of Cloud Computing
 - 252.239-7010 Cloud Computing Services
 - Frequently Asked Questions
- **Guidance to Stakeholders** (<http://www.acq.osd.mil/se/docs/DFARS-guide.pdf>)
- **NIST SP 800-171** (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>)
- **Cloud Computing Security Requirements Guide (SRG)**
(http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf)





Questions?





Back Up

- **NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**





NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

- **Developed for use on contractor and other nonfederal information systems to protect CUI (*published June 2015*)**
 - Replaces use of selected security controls from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations in original DFARS Clause 252.204-7012 (*circa November 18, 2013*)
- **Enables contractors to comply using systems and practices already in place**
 - Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI
 - Requirements are performance-based, significantly reduce unnecessary specificity, and are more easily applied to existing systems.
- **Provides standardized/uniform set of requirements for all CUI security needs**
 - Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers)
 - Allows contractor to implement alternative, but equally effective, security measures to satisfy every CUI security requirement



Structure of NIST SP 800-171 Security Requirements

800-171 security requirements have a well-defined structure with the following components:

- **Basic security requirements section.**
 - Essentially FIPS 200 requirements applicable to protection of CUI
- **Derived security requirements section.**
 - “Derived” from NIST 800-53 moderate baseline controls that are applicable to protection of CUI
 - Includes only the essentials – most ‘procedural’ elements have been eliminated

Replacing NIST SP 800-53 based controls with NIST SP 800-171

Derived Security Requirement:

- Most substantial addition is requirement for **multifactor authentication**
- **NOT** a requirement to use PIV/CAC, but any method described in NIST SP 800-63-2, Electronic Authentication Guideline (e.g., password plus cell-phone txt message)

Annex D, Mapping Tables

- Maps 800-171 requirements to 800-53 and ISO/IEC 27001 controls
- **INFORMATIONAL ONLY**– tables NOT intended to convey or impart ANY additional CUI security requirements beyond Basic/Derived requirements in Chapter 3
- **Agencies shall NOT require the mapped 800-53 control**
 - **The 800-171 Basic or Derived Requirement IS the requirement**
- Agencies may, in special circumstances, require additional security controls and then reference an additional 800-53 control
 - Additional control should NOT be a control included in the mapping table

Annex E, Tailoring Tables

- Provides rationale for not including a 800-53 moderate control in 800-171
- **NFO: Expected to be routinely satisfied by Nonfederal Org without specification** – agencies may ask ‘how’ these are implemented by the contractor (e.g., “what mechanisms does the company employ to ensure requirement xx is properly implemented and sustained?”)

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
<p>3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</p> <p>3.1.2 Limit information system access to the types of transactions and functions authorized users are permitted to execute.</p>	<p>AC-2 ACCOUNT MANAGEMENT <u>The organization:</u></p> <ul style="list-style-type: none">a. Identifies/selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];b. Assigns account managers for information system accounts;c. Establishes conditions for group and role membership;d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];g. Monitors the use of, information system accounts;h. Notifies account managers:<ul style="list-style-type: none">1. When accounts are no longer required;2. When users are terminated or transferred; and3. When individual information system usage or need-to-know changes;i. Authorizes access to the information system based on:<ul style="list-style-type: none">1. A valid access authorization;2. Intended system usage; and3. Other attributes as required by the organization or associated missions/business functions;j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; andk. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. <p>AC-3 ACCESS ENFORCEMENT <u>The information system</u> enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.</p> <p>AC-17 REMOTE ACCESS <u>The organization:</u></p> <ul style="list-style-type: none">a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; andb. Authorizes remote access to the information system prior to allowing such connections. <p style="text-align: center;">Unclassified</p>

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
<p>3.8.9 Protect the confidentiality of backup CUI at storage locations.</p>	<p>CP-9 INFORMATION SYSTEM BACKUP <u>The organization:</u></p> <ul style="list-style-type: none">a. Conducts backups of user-level information contained in the information system [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>];b. Conducts backups of system-level information contained in the information system [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>];c. Conducts backups of information system documentation including security-related documentation [<i>Assignment: organization-defined frequency consistent with recovery time and recovery point objectives</i>]; andd. Protects the confidentiality, integrity, and availability of backup information at storage locations.
<p>3.5.5 Prevent reuse of identifiers for a defined period.</p> <p>3.5.6 Disable identifiers after a defined period of inactivity.</p>	<p>IA-4 IDENTIFIER MANAGEMENT <u>The organization manages information system identifiers by:</u></p> <ul style="list-style-type: none">a. Receiving authorization from [<i>Assignment: organization-defined personnel or roles</i>] to assign an individual, group, role, or device identifier;b. Selecting an identifier that identifies an individual, group, role, or device;c. Assigning the identifier to the intended individual, group, role, or device;d. Preventing reuse of identifiers for [<i>Assignment: organization-defined time period</i>]; ande. Disabling the identifier after [<i>Assignment: organization-defined time period of inactivity</i>].

Replacing NIST SP 800-53 based controls with NIST SP 800-171

NIST SP 800-171 Requirement	NIST SP 800-53 Requirement (from DFARS Table 1)
<p>3.10.3 Escort visitors and monitor visitor activity.</p> <p>3.10.4 Maintain audit logs of physical access</p> <p>3.10.5 Control and manage physical access devices</p>	<p>PE -3 PHYSICAL ACCESS CONTROL <u>The organization:</u></p> <p>a. Enforces physical access authorizations at [<i>Assignment: organization-defined entry/exit points to the facility where the information system resides</i>] by;</p> <p>1. Verifying individual access authorizations before granting access to the facility; and</p> <p>2. Controlling ingress/egress to the facility using [<i>Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards</i>];</p> <p>b. Maintains physical access audit logs for [<i>Assignment: organization-defined entry/exit points</i>];</p> <p>c. Provides [<i>Assignment: organization-defined security safeguards</i>] to control access to areas within the facility officially designated as publicly accessible;</p> <p>d. Escorts visitors and monitors visitor activity [<i>Assignment: organization-defined circumstances requiring visitor escorts and monitoring</i>];</p> <p>e. Secures keys, combinations, and other physical access devices;</p> <p>f. Inventories [<i>Assignment: organization-defined physical access devices</i>] every [<i>Assignment: organization-defined frequency</i>]; and</p> <p>g. Changes combinations and keys [<i>Assignment: organization-defined frequency</i>] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.</p>