TAB P

Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
Incorporating Change 2, July 28, 2017

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and

all other organizational entities within the Department of Defense (referred to collectively in this instruction as the "DoD Components").

(2) The United States Coast Guard. The United States Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this instruction in accordance with the direction in Paragraphs 4a, b, c, and d of the Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security (Reference (q)).

~~(2)~~*(3)* All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products. This includes IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD.

b. Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI), as directed by Executive Order 12333 (Reference (l)) and other laws and regulations. The application of the provisions and procedures of this instruction to information technologies processing SCI is encouraged where they may complement or cover areas not otherwise specifically addressed.

3. <u>POLICY</u>. It is DoD policy that:

a. The DoD will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF) that includes and integrates DoD mission areas (MAs) pursuant to DoDD 8115.01 (Reference (m)) and the governance process prescribed in this instruction.

b. The cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Reference (c)). DoD IS and PIT systems will transition to the RMF in accordance with Table 2 of Enclosure 8 of this instruction.

c. The RMF must satisfy the requirements of subchapter III of chapter 35 of Title 44, United States Code (U.S.C.), also known and referred to in this instruction as the "Federal Information Security Management Act (FISMA) of 2002" (Reference (d)). DoD must meet or exceed the standards required by the Office of Management and Budget (OMB) and the Secretary of Commerce, pursuant to FISMA and section 11331 of Title 40, U.S.C. (Reference (n)).

d. All DoD IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253 (Reference (e)), implement a corresponding set of security controls from NIST SP 800-53 (Reference (f)), and use assessment procedures from NIST SP 800-53A (Reference (g)) and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the Knowledge Service (KS) at https://rmfks.osd.mil. As supporting reference security control documents are updated, DoD's implementation of these updates will be coordinated through the RMF TAG.

e. Resources for implementing the RMF must be identified and allocated as part of the Defense planning, programming, budgeting, and execution process.

f. Each DoD IS, DoD partnered system, and PIT system must have an authorizing official (AO) responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture.

g. Reciprocal acceptance of DoD and other federal agency and department IS and PIT system authorizations will be implemented to the maximum extent possible. Refusals must be timely, documented, and reported to the responsible DoD Component senior information security officer (SISO) (formerly known as the senior information assurance (IA) officer).

h. All DoD IT identified in paragraph 2a(2) must be under the governance of a DoD Component cybersecurity program in accordance with DoDI 8500.01(Reference (h)).

i. A plan of action and milestones (POA&M) must be developed and maintained to address known vulnerabilities in the IS or PIT system.

j. Continuous monitoring capabilities will be implemented to the greatest extent possible.

k. The RMF process will inform acquisition processes for all DoD IT, including requirements development, procurement, and both developmental T&E (DT&E) and operational T&E (OT&E), but does not replace these processes.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release.** This instruction is available on ~~the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ *the Directives Division Website at http://www.esd.whs.mil/DD/.*

7. EFFECTIVE DATE. This instruction is effective March 12, 2014.

Teresa M. Takai
DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. RMF Procedures
4. RMF Governance
5. Cybersecurity Reciprocity
6. Risk Management of IS and PIT Systems
7. KS
8. RMF Transition

Glossary

TABLE OF CONTENTS

TABLES

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007 (hereby cancelled)

(b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014

(c) National Institute of Standards and Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010, as amended

(d) Subchapter ~~III~~ *II* of chapter 35 of Title 44, United States Code (also known as the "Federal Information Security ~~Management~~ *Modernization* Act (FISMA) of ~~2002~~ *2014*")

(e) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," ~~March 15, 2012~~ *March 27, 2014*, as amended

(f) National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," current edition

(g) National Institute of Standards and Technology Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," June 2010, as amended

(h) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

(i) National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011

(j) National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," September 2012, as amended

(k) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016

(l) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

(m) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005

(n) Section 11331 of Title 40, United States Code

(o) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015

(p) DoD Instruction 8581.01, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 8, 2010

(q) DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department Of Defense," August 3, 2015

(r) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 27, 2015*, as amended*

(s) DoD Chief Information Officer Memorandum, "DoD Enterprise Services Designation – Collaboration, Content Discovery, and Content Delivery," February 2, 2009

(t) DoD Chief Information Officer and Intelligence Community Chief Information Officer Memorandum, "Use of Unified Cross Domain Management Office (UCDMO) Baseline Cross Domain Solutions (CDSs)," December 1, 2011

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO:

a. Oversees implementation of this instruction, directs and oversees the cybersecurity risk management of DoD IT, distributes RMF information standards and sharing requirements, and manages the transition from the DIACAP to the RMF.

b. In coordination with the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) and the Director, Operational Test and Evaluation (DOT&E), ensures developmental and OT&E activities and findings are integrated into the RMF.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO *and in addition to the responsibilities in paragraph 7 of this enclosure*, the Director, DISA:

a. Ensures control correlation identifiers (CCIs), security requirements guides (SRGs), and security technical implementation guides (STIGs) developed by DISA are consistent with security controls and assessment procedures used by the DoD.

b. Develops and provides RMF training and awareness products and a distributive training capability to support the DoD Components in accordance with Reference (h) and DoDD 8140.01 (Reference (o)); posts the training materials on the IA Support Environment Website (http://iase.disa.mil).

c. Identifies or develops and provides DoD Enterprise RMF management tools.

3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) coordinates with the DoD CIO to ensure RMFs processes are appropriately integrated with Defense Acquisition System processes for acquisitions of DoD IT.

4. DASD(DT&E). Under the authority, direction, and control of the USD(AT&L), the DASD(DT&E), in coordination with the DoD CIO, ensures integration of DT&E activities into the RMF and provides the RMF TAG with input as appropriate or required.

5. DOT&E. The DOT&E:

a. Reviews plans, execution, and results of operational testing to ensure adequate evaluation of cybersecurity for all DoD IT acquisitions subject to oversight.

b. In coordination with DoD CIO, ensures integration of OT&E activities into the RMF and provides the RMF TAG with input as appropriate or required.

6. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS)). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence *and in addition to the responsibilities in paragraph 7 of this enclosure*, the DIRNSA/CHCSS:

a. Ensures IS security engineering services, when provided to the DoD Components, support the RMF.

b. Develops risk model and risk assessment tools to support authorization decisions.

7. DoD COMPONENT HEADS. The DoD Components heads:

a. Ensure DoD IS and PIT systems are categorized according to the guidelines provided in this instruction.

b. Verify that a program manager (PM) or system manager (SM) is appointed for all ISs and PIT systems.

c. Ensure a trained and qualified AO is appointed in writing for all DoD IS and PIT systems operating within or on behalf of the DoD Component in accordance with Reference (h) and that the systems are authorized in accordance with this instruction.

(1) This role must be assigned to government personnel only. This role may not be re-delegated to personnel that do not also meet these requirements.

(2) Relevant PIT expertise must be a factor in the selection and appointment of AOs responsible for authorizing PIT systems.

d. Develop and issue guidance for PIT systems that reflects DoD Component-unique operational and environmental demands as needed.

e Ensure DoD information technologies under their authority comply with the RMF.

f. Operate only authorized ISs and PIT systems (i.e., those with a current authorization to operate (ATO) or interim authorization to test (IATT)).

g. Comply with all authorization decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATD).

h. Ensure personnel engaged in or supporting the RMF are appropriately trained and possess professional certifications consistent with Reference (o) and supporting issuances.

i. Ensure IS owners (ISOs) appoint user representatives (URs) for DoD IS and PIT systems under the DoD Component's purview.

j. Oversee the DoD Component chief information officer (CIO)'s implementation of this instruction.

k. Ensure participation in the RMF TAG.

l. Ensure that contracts and other agreements include specific requirements in accordance with this instruction.

8. CJCS. In coordination with the DoD CIO *and in addition to the responsibilities in paragraph 7 of this enclosure*, the CJCS ensures the Joint Capabilities Integration and Development System (JCIDS) process supports and documents IS and PIT system categorization consistent with this instruction.

9. COMMANDER, U.S. STRATEGIC COMMAND (USSTRATCOM). *In addition to the responsibilities in paragraph 7 of this enclosure* The Commander, USSTRATCOM:

a. Assigns AOs, issues authorization guidance consistent with this instruction, and resolves authorization issues for space systems used by the DoD in accordance with DoDI 8581.01 (Reference (p)).

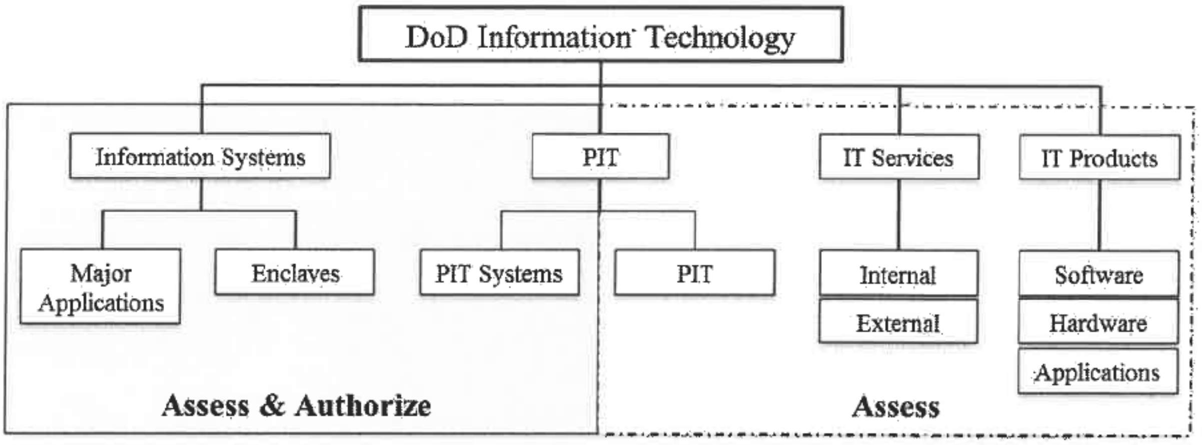
b. Serves as the AO for authorizing the processing, storing, or transmitting of nuclear command, control, and communication data on ISs.

ENCLOSURE 3

RMF PROCEDURES

1. OVERVIEW. The forms of DoD IT, as shown in Figure 1, range in size and complexity from individual hardware and software products to stand-alone systems to massive computing environments, enclaves, and networks.

Figure 1. DoD IT



2. RISK MANAGEMENT OF IS AND PIT SYSTEMS. See Enclosure 6.

3. RISK MANAGEMENT OF IT PRODUCTS, SERVICES, AND PIT. IT products, services, and PIT are not authorized for operation through the full RMF process. These types of IT must be securely configured in accordance with applicable DoD policies and security controls and undergo special assessment of their functional and security-related capabilities and deficiencies. The IS security manager (ISSM) (with the review and approval of the responsible AO) is responsible for ensuring all products, services and PIT have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system. Paragraphs 3a through 3c summarize the categories of IT, the applicable evaluation process, and associated policy references.

a. IT Products. IT products (including applications), as defined in Reference (h), will be configured in accordance with applicable STIGs under a cognizant ISSM and security control assessor (SCA). STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. SRGs are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used. STIGs, SRGs and CCIs are available on the IA Support Environment Website (http://iase.disa.mil). STIG and SRG compliance results for products will be documented as security control assessment results within a product-level security assessment report (SAR) and reviewed by the responsible ISSM (under the direction of the AO) prior to acceptance or connection into an authorized computing environment (e.g., an IS or PIT system with an authorization). This review ensures products will not introduce vulnerabilities into the hosting IS or PIT system. DoD Component-level guidance maximizes testing and review results to minimize duplication of effort across the DoD. See the KS for additional guidance on the review of products.

b. IT Services. IT services are outside the service user organization's authorization boundary, and the service user's organization has no direct control over the application or assessment of required security controls. DoD organizations that use IT services are typically not responsible for authorizing them (i.e., issue an authorization decision).

(1) Internal IT services are delivered by DoD ISs. DoD organizations that use internal IT services must ensure the categorization of the IS delivering the service is appropriate to the needs of the DoD IS using the service, and that written agreements describing the roles and responsibilities of both the providing and the receiving organization are in place.

(2) DoD organizations that use external IT services provided by a non-DoD federal government agency must ensure the categorization of the IS delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission, and that the IS delivering the service is operating under a current authorization from that agency. In accordance with Reference (h), interagency agreements or government statements of work for these external services must contain requirements for service level agreements (SLAs) that include the application of appropriate security controls.

(3) DoD organizations that use external IT services provided by a commercial or other non-federal government entity must ensure the security protections of the IS delivering the service is appropriate to the confidentiality, integrity, and availability needs of the DoD organization's information and mission. DoD organizations must perform categorization in accordance with Reference (e) and tailor appropriately to determine the set of security controls to be included in requests for proposals. DoD organizations will assess the adequacy of security proposed by potential service providers, and accept the proposed approach, negotiate changes to the approach to meet DoD needs, or reject the offer. The accepted security approach must be documented in the resulting contract or order.

(4) DoD organizations contracting for external IT services in the form of commercial cloud computing services must comply with DoD cloud computing policy and procedural guidance as published.

c. PIT. PIT that does not rise to the level of a PIT System may be categorized using Reference (e) with the resultant security control baselines tailored as needed. Otherwise, the specific cybersecurity needs of PIT must be assessed on a case-by-case basis and security controls applied as appropriate.

exchanges and connections for enterprise ISs, cross-MA ISs, cross security domain connections, and mission partner connections.

(b) Defense~~-IA~~ Security/*Cybersecurity* ~~Accreditation~~ *Authorization* Working Group (DSAWG). The DSAWG, in support of the DoD ISRMC, is the community forum for reviewing and resolving authorization issues related to the sharing of community risk. The DSAWG develops and provides guidance to the AOs for IS connections to the DoD Information Enterprise.

(3) DoD SISO. The DoD SISO, in accordance with Reference (h), represents the DoD CIO and directs and coordinates the DoD Cybersecurity Program, which includes the establishment and maintenance of the RMF. In addition, the DoD SISO:

(a) Advises and informs the principal authorizing officials (PAOs) and their representatives.

(b) Oversees the RMF TAG and the online KS.

(4) DoD Cybersecurity Architecture. The DoD Cybersecurity architecture consists of strategies, standards, and plans that have been developed for achieving an assured, integrated, and survivable information enterprise.

(5) The RMF TAG. The RMF TAG (formerly known as the DIACAP TAG) provides implementation guidance for the RMF by interfacing with the DoD Component cybersecurity programs, cybersecurity communities of interest (COIs), and other entities (e.g., DSAWG) to address issues that are common across all entities, by:

(a) Providing detailed analysis and authoring support for the KS.

(b) Recommending changes to security controls in Reference (f), security control baselines and overlays in Reference (e), DoD assignment values, and associated implementation guidance and assessment procedures to the DoD CIO.

(c) Recommending changes to cybersecurity risk management processes to the DoD CIO.

(d) Advising DoD forums established to resolve RMF priorities and cross-cutting issues.

(e) Developing and managing automation requirements for DoD services that support the RMF.

(f) Developing guidance for facilitating RMF reciprocity throughout the DoD.

(6) The KS. The KS, a dynamic online knowledge base, supports RMF implementation, planning, and execution by functioning as the authoritative source for RMF procedures and

guidance. The KS supports RMF practitioners by providing access to DoD security control baselines, security control descriptions, security control overlays, and implementation guidance and assessment procedures, all compliant with References (e) and (f). The KS also supports the RMF TAG by enabling TAG functions and activities, including maintenance of membership; voting, analysis, and authoring; and configuration control of KS enterprise content and functionality. See Enclosure 7 for more information on KS capabilities.

b. Tier 2 - Mission/Business Processes

(1) PAO. A PAO is appointed for each of the DoD MAs (i.e., the warfighting MA (WMA), business MA (BMA), enterprise information environment MA (EIEMA), and DoD portion of the intelligence MA (DIMA)), and their representatives are members of the DoD ISRMC. PAOs must:

(a) Represent the interests of the MA, as defined in Reference (m), and, as required, issues authorization guidance specific to the MA, consistent with this instruction.

(b) Resolve authorization issues within their respective MAs and work with other PAOs to resolve issues among MAs, as needed.

(c) Designate AOs for MA IS and PIT systems supporting MA COIs specified in DoDI 8320.07 (Reference (q)), in coordination with appropriate DoD Component heads, if required.

(d) Designate information security architects or IS security engineers for MA segments or systems of systems, as needed.

(2) DoD Component CIO. Each DoD Component CIO, supported by the DoD Component SISO appointed in accordance with Reference (h), is responsible for administration of the RMF within the DoD Component cybersecurity program; participation in the RMF TAG; visibility and sharing of the RMF status of assigned ISs and PIT systems; and enforcement of training requirements for persons participating in the RMF. DoD Component CIOs must:

(a) Maintain visibility of assessment and authorization status of DoD Component IS and PIT systems through automated assessment and authorization tools or designated repositories for their Component to the DoD CIO and PAOs.

(b) Verify that a PM or SM is identified for each DoD Component IS and PIT system.

(c) Establish and maintain processes and procedures to manage DoD Component POA&Ms.

(d) Appoint a DoD Component SISO to direct and coordinate the DoD Component cybersecurity program.

(e) Review and document concurrence on all ATOs issued for Component IS and PIT systems with a level of risk of "Very High" or "High."

(3) DoD Component SISO. DoD Component SISOs have authority and responsibility for security controls assessment and must establish and manage a coordinated security assessment process for information technologies governed by the DoD Component cybersecurity program. DoD Component SISOs must:

(a) Implement and enforce the RMF within the DoD Component cybersecurity program.

(b) Perform as the SCA or formally delegate the security control assessment role for governed information technologies.

(c) Track the assessment and authorization status of IS and PIT systems governed by the DoD Component cybersecurity program.

(d) Establish and oversee a team of cybersecurity professionals qualified in accordance with Reference (p), responsible for conducting security assessments. DoD Component SISOs may task, organize, staff, and centralize or direct assessment activities to representatives as appropriate. Regardless of the adopted model, the SISO is responsible for assessing quality, capacity, visibility, and effectiveness.

(e) Identify and recommend changes and improvements to the security assessment process, security T&E, and risk assessment methodology, including procedures, risk factors, assessment approach, and analysis approach to the RMF TAG for inclusion in the KS.

(f) Advise AOs on the adequacy of acquisition program implementation of cybersecurity requirements.

(g) Serve as the single cybersecurity coordination point for joint or DoD-wide programs that are deploying information technologies to DoD Component enclaves.

(h) Ensure DoD Component RMF guidance is posted to the DoD Component portion of the KS, and is consistent with DoD policy and guidance.

(i) Oversee DoD Component-level participation in the RMF TAG.

c. Tier 3 – IS and PIT Systems

(1) AO. The DoD Component heads are responsible for the appointment of trained and qualified AOs for all DoD ISs and PIT systems within their Component. AOs should be appointed from senior leadership positions within business owner and mission owner organizations (as opposed to limiting appointments to CIO organizations) to promote accountability in authorization decisions that balance mission and business needs and security concerns. In addition to the responsibilities established in Reference (h), AOs must:

(a) Comply with DoD ISRMC direction issued on behalf of the MA PAOs.

(b) Ensure all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned ISs and PIT systems.

(c) Monitor and track overall execution of system-level POA&Ms.

(d) Promote reciprocity to the maximum extent possible.

(e) Not delegate authorization decisions. Other AO responsibilities and tasks may be delegated to formally appointed and qualified AO designated representatives (AODRs).

(2) IS or PIT System Cybersecurity Program. The system cybersecurity program consists of the policies, procedures, and activities of the ISO, PM/SM, UR, ISSM, and IS security officers (ISSOs) at the system level. The system cybersecurity program implements and executes policy and guidance from Tier 1 and Tier 2, and augments them as needed. The system cybersecurity program is responsible for establishing and maintaining the security of the system, including the monitoring and reporting of the system security status. Specific cybersecurity program responsibilities include:

(a) ISOs must:

1. In coordination with the information owner (IO), categorize systems in accordance with Reference (e) and document the categorization in the appropriate JCIDS capabilities document (e.g., capabilities development document).

2. Appoint a UR for assigned IS and PIT systems.

3. Develop, maintain, and track the security plan for assigned IS and PIT systems. (Common security controls owner performs this function for inherited controls.)

(b) PMs (or SM, if no PM is assigned) must:

1. Appoint an ISSM for each assigned IS or PIT system with the support, authority, and resources to satisfy the responsibilities established in this instruction.

2. Ensure each program acquiring an IS or PIT system has an assigned IS security engineer and that they are fully integrated into the systems engineering process.

3. Implement the RMF for assigned IS and PIT systems.

4. Ensure the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

5. Enforce AO authorization decisions for hosted or interconnected IS and PIT systems.

6. Implement and assist the ISO in the maintenance and tracking of the security plan for assigned IS and PIT systems.

7. Ensure POA&M development, tracking, and resolution.

8. Ensure periodic reviews, testing and assessment of assigned IS and PIT systems are conducted at least annually.

9. Provide the IS or PIT system description.

10. Register the IS or PIT system in the DoD Component registry.

11. Ensure T&E of assigned IS and IT system is planned, resourced, and documented in the program T&E master plan in accordance with DoDI 5000.02 (Reference (r)).

(c) URs must represent the operational and functional requirements of the user community in the RMF process.

(d) ISSMs, in addition to the responsibilities established in Reference (h), must:

1. Support implementation of the RMF.

2. Maintain and report IS and PIT systems assessment and authorization status and issues in accordance with DoD Component guidance.

3. Provide direction to the ISSO in accordance with Reference (h).

4. Coordinate with the organization's security manager to ensure issues affecting the organization's overall security are addressed appropriately.

2. RMF ROLE APPOINTMENT. Table 1 identifies the appropriate authority for the appointment of RMF roles.

Table 1. Appointment of RMF Roles

Role	Appointed By
PAO (formerly principal accrediting authority)	DoD MA owner
DoD SISO (formerly the Senior IA Officer)	DoD CIO
DoD Component CIO	DoD Component head
AO (formerly designated approving (or accrediting) authority)	DoD Component head; PAO for MA-managed ISs
AODR (formerly designated approving (or accrediting) authority representative)	AO
DoD Component SISO	DoD Component CIO or, in organizations in which the position of DoD Component CIO does not exist, the DoD Component head.
SCA (formerly certifying authority)	DoD Component SISO is the Component SCA, but may formally delegate the SCA role as appropriate.
PM/SM	DoD Component head
ISSM (formerly IA manager)	PM or SM
UR	ISO
RMF TAG Representative (formerly DIACAP TAG Representative)	DoD Component SISO

ENCLOSURE 5

CYBERSECURITY RECIPROCITY

1. Cybersecurity reciprocity (referred to in this instruction as "reciprocity") is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation. In order to facilitate reciprocity, the concepts in paragraphs 1a through 1e are fundamental to a common understanding and must be adhered to:

a. IS and PIT systems have only a single valid authorization. Multiple authorizations indicate multiple systems under separate ownership and configuration control.

b. Deploying systems with valid authorizations (from a DoD organization or other federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site. Deploying system ISOs and PMs must coordinate system security requirement with receiving organizations or their representatives early and throughout system development.

c. An authorization decision for IS or PIT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations. PMs/ ISOs deploying systems across DoD Components will post security authorization documentation to Enterprise Mission Assurance Support Service (eMASS) or other electronic means to provide visibility of authorization status and documentation to planned receiving sites.

d. The process for receiving organization to accept IS and PIT systems is:

(1) Review the complete security authorization package.

(2) Determine the security impact of connecting the deploying system within the receiving enclave or site.

(3) Determine the risk of hosting the deploying system within the enclave or site.

(4) If the risk is acceptable, execute a documented agreement between deploying and receiving organizations (e.g., memorandum of understanding (MOU), memorandum of agreement (MOA), SLA) for the maintenance and monitoring of the security posture of the system (security controls, ~~computer network defense~~ *cybersecurity* service provider (~~CNDSP~~ *CSSP*), etc.).

(5) Document the acceptance by the receiving AO.

(6) Update the receiving enclave or site authorization documentation for inclusion of the deployed system.

e. Receiving organizations have the right to refuse deploying systems due to a security authorization package that does not meet sufficiency and completeness requirements as defined on the KS, or excessive risk to the enclave or site, as determined by the enclave or site AO. Refusals must be documented by the refusing AO, and provided to the deploying organization's ISO or PM, AO, and Component SISO, and to the refusing organization's Component SISO. Disputes should be resolved at the lowest possible level. Disputes that cannot be resolved will be raised to the next appropriate level (e.g., DoD Component, MA PAO, DSAWG, DoD ISRMC).

2. The cases in paragraph 2a through 2e describe the proper application of DoD policy on reciprocity in the most frequently occurring scenarios:

a. A system is authorized by a DoD AO for subsequent deployment into receiving environments authorized by other DoD AOs. This case includes systems designated as enterprise systems in accordance with DoD CIO Memorandum (Reference (s)), as well as non-enterprise systems that will be developed, authorized, and deployed within a single DoD Component, or across multiple DoD Components. Systems with existing authorizations issued by DoD AOs do not require a new authorization to be issued by the receiving enclave or site.

(1) The receiving site executes the acceptance process in paragraph 1d of this enclosure. Issues identified during the acceptance process will be negotiated between the deploying ISO or PM and the receiving enclave or site ISO or SM. Following resolution of any issues, which may result in modifications in either the deploying system or the receiving environment, the deploying system is allowed to be incorporated or connected to the hosting environment. The nature or magnitude of any modifications to the deploying system or receiving site may result in additional assessment activities, but the deploying system and receiving environment retain their own separate authorizations. It is the joint responsibility of the ISOs of deploying systems and the receiving sites to ensure the system design reflects the security, technical and threat environment of the planned receiving sites, as well as leveraging any common controls. Unresolved issues, disputes, and refusals are addressed in accordance with paragraph 1e of this enclosure. Document the acceptance by the receiving AO.

(2) The DoD ISRMC, supported by the DSAWG, may make an enterprise level risk acceptance determination for authorized enterprise systems, which will satisfy the requirements of the first three elements of paragraph 1d of this enclosure. If the DoD ISRMC accepts the risk on behalf of the DoD Information Enterprise, the receiving organization may not refuse to deploy the system.

b. A system is authorized by another U.S. Government agency, and a DoD organization takes ownership of the system for deployment into DoD ISs or enclaves. Systems with an existing authorization issued by other federal agencies require authorization by a DoD AO in accordance with Enclosure 3 of this instruction prior to operating if the providing organization relinquishes configuration and maintenance of the system to the DoD. The receiving enclave or site will maximize reuse of the external agency's security authorization package to support the authorization by the DoD AO. Following the issuance of a DoD authorization, subsequent deployment of the system by the DoD ISO or PM to DoD receiving sites will follow the review and acceptance process described in paragraph 1d of this enclosure.

c. A system is authorized by a DoD organization for its own use, and subsequently provided to another DoD organization for it to use as a separately owned, managed and maintained system. In this case, the receiving organization becomes the ISO and must authorize the system in accordance with Enclosure 3 of this instruction. The receiving enclave or site will maximize reuse of the existing authorization documentation to support the authorization by the receiving AO. Following the issuance of the authorization, subsequent deployment of the system by the system owner to other receiving sites will follow the review and acceptance process described in paragraph 1d of this enclosure.

d. A DoD system is authorized and subsequently deployed for acceptance into receiving sites authorized by a U.S. Government agency other than DoD. In this case, the DoD system's security authorization documentation is made available to the receiving U.S. Government agency. If the receiving agency determines there is insufficient information in the documentation or inadequate security measures in place for establishing an acceptable level of risk, the receiving agency may negotiate with the deploying DoD organization for additional security measures or security-related information. The additional security measures or security-related information may be provided by the DoD organization, the system developer, the receiving agency, some other external third party, or some combination of the above.

e. A DoD organization plans to use an IT service under contract from a commercial entity that has been authorized by a DoD or other U.S. Government agency (e.g., a commercial cloud service authorized by the Federal Risk and Authorization Management Program Joint Authorization Board). In this case, the DoD organization leverages an existing authorization, and maximizes reuse of the existing authorization documentation to support a new authorization by a DoD AO. If the DoD organization determines there are inadequate security measures in place for establishing an acceptable level of risk, the DoD organization may negotiate with IT service provider for additional security measures or security-related information. Upon assessment and approval of all newly included security measures and the documentation of all applicable security measures in the contract agreement with the IT service provider, the DoD organization AO issues an authorization.

ENCLOSURE 6

RISK MANAGEMENT OF IS AND PIT SYSTEMS

1. OVERVIEW. This enclosure describes the DoD process for identifying, implementing, assessing, and managing cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of IS and PIT systems. This enclosure is designed to be a companion guide to Reference (c), providing specific guidance for implementation within DoD. DoD personnel serving in RMF roles at every level should refer to Reference (c) for a full description of the process, definitions, roles and responsibilities, and activities. In cases where Reference (c) conflicts with this instruction, compliance with this instruction takes precedence and is required. The KS also provides expanded coverage of this subject, as well as tools, templates, and best practice information.

a. Applicability. This process is applicable to all IS and PIT systems, as well as DoD partnered systems where it has been agreed that DoD standards will be followed. IT below the system level (e.g., products, IT services) will not be subjected to the full process described in this enclosure. However, IT below the system level must be securely configured (in accordance with applicable DoD policies and security controls), documented in the authorization package and reviewed by the responsible ISSM (under the direction of the AO) for acceptance or connection into an authorized computing environment (i.e., an authorized IS or PIT system).

b. Considerations for Special System Configurations

(1) IS and PIT Systems Implementing a cross domain solution (CDS). CDSs are typically deployed within the IS or PIT system authorization boundary on the system with the higher classification of the cross domain connection, and are included in the IS or PIT system authorization. The AO responsible for the IS or PIT system must consider the security impact of the CDS operation in the overall authorization decision. In addition to the high-side security requirements and ATO, the security requirements for the integrity of the information transfer must be considered and implemented on the connecting low-side IS(s). Additional detail and authoritative guidance is provided in DoD CIO and Intelligence Community CIO Memorandum (Reference (t)) and CJCS Instruction 6211.02D (Reference (u)).

(2) ISs and PIT Systems Providing Unified Capabilities (UC). DoDI 8100.04 (Reference (v)) contains DoD policy for UC, and describes the process for the ~~IA~~ *cybersecurity* certification of UC products. UC products are implemented inside the authorization boundaries of DoD ISs, and the UC product ~~IA~~ *cybersecurity* certification documentation is used to support the overall system assessment and authorization.

(3) Type Authorization. The type authorization is used to deploy identical copies of an IS or PIT system in specified environments. This method allows a single security authorization package to be developed for an archetype (common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave.

(4) Stand-Alone IS and PIT System. Stand-alone IS and PIT systems are types of enclaves that are not interconnected to any other network. Stand-alone IS and PIT systems do not transmit, receive, route, or exchange information outside of the system's authorization boundary. They may range in size from a single workstation to multiple interconnected subsystems as long as they meet the foregoing criteria. Stand-alone IS and PIT systems are authorized as any other IS and PIT systems, but assigned security control sets may be tailored as appropriate with the approval of the AO (e.g., network-related controls may be eliminated). Stand-alone IS and PIT systems must always be clearly identified as such in the authorization documentation. Additionally, identical stand-alone IS and PIT systems that have identical security control implementation and are to be deployed to multiple locations may be type authorized.

(5) DoD-Controlled IS and PIT Systems Operated by a Contractor or Other Entity on Behalf of the DoD. Externally owned IS and PIT systems that are dedicated to DoD processing and are effectively under DoD configuration control must be authorized as DoD IS and PIT systems. A DoD AO must render an authorization decision for this type of a DoD system prior to DoD use of the capability. The following additional requirements apply:

(a) Security responsibilities of the service provider down to the control level must be made explicit in the contract or other binding agreement, along with any other performance and service-level parameters by which the DoD entity will measure the cybersecurity performance of the system for the purpose of authorization.

(b) Technical security of the outsourced environment must be the responsibility of the service provider.

(c) Responsibility for procedural and administrative security will be shared between the service provider and the supported DoD entity contracting for the service.

(d) Security requirements for such a system must be determined by the categorization and control selection process described in paragraphs 2a and 2b of this enclosure, just as for other DoD ISs. Any required security controls that are not explicit in the contract or otherwise covered by a SLA must be assessed as non-compliant (NC). All such NC security controls must be documented in a POA&M with an explanation as to why accepting the risk of operating the system with that control in an NC status is acceptable.

(6) DoD Partnered Systems. DoD partnered systems are ISs or PIT systems that are developed jointly by DoD and non-DoD mission partners, comprise DoD and non-DoD ISs, or contain a mix of DoD and non-DoD information consumers and producers, (e.g., jointly developed systems, multi-national or coalition environments, or first responder environments). Security control selection, system authorization, and other risk management considerations for DoD partnered systems must be clearly defined via a formal partnership agreement, e.g., an MOA, MOU, or SLA. To the extent possible, the negotiated risk management approach should be aligned with the RMF. Regardless of the risk management approach employed, a DoD AO

must render an authorization decision for a DoD partnered system prior to DoD use of the capability.

(7) OSD Systems. Pursuant to DoDD 5105.53 (Reference (w)), the Director of Administration, Office of the Deputy Chief Management Officer of the Department of Defense, is responsible for the IT, including IS and PIT systems, supporting the OSD staff in the National Capital Region.

c. Authorization Approaches. Reference (c) describes three different approaches when planning for and conducting security authorizations. DoD Components may employ any of the following approaches for the authorization of IS and PIT systems:

(1) Authorization with a Single AO. This is the traditional authorization process defined in this enclosure, where a single official in a senior leadership position is both responsible and accountable for a system. The official also accepts the system-related security risks that may impact organizational operations and assets, individuals, other organizations, or the Nation.

(2) Authorization with Multiple AOs. This approach, also known as a joint authorization, is employed when multiple officials either from the same or different organizations, have a shared interest in authorizing a system.

(a) The AOs collectively are responsible and accountable for the system and jointly accept the system-related security risks that may adversely impact organizational operations and assets, individuals, other organizations, and the Nation.

(b) A similar authorization process is followed as with an authorization by a single AO, with the essential difference being the addition of multiple AOs.

(c) Organizations choosing a joint authorization approach are expected to work together on the planning and the execution of RMF tasks, and to formally document their agreement and progress in implementing the tasks. Collaborating on the security categorization, selection of security controls, plan for assessing the controls to determine effectiveness, POA&Ms, and system-level continuous monitoring strategy, is necessary for a successful joint authorization.

(d) The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization, including for example, the process for ongoing determination and acceptance of risk.

(e) The joint authorization remains in effect only as long as there is mutual agreement among AOs and the authorization meets the requirements established by federal or organizational policies.

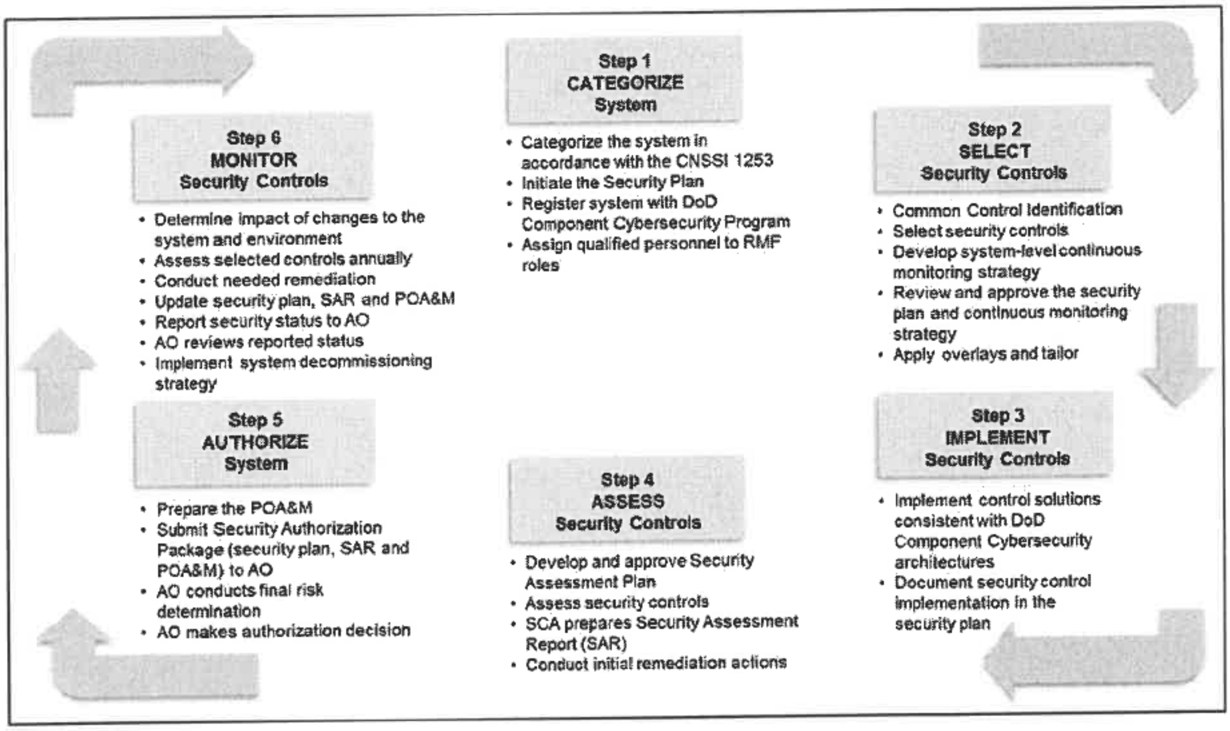
(3) Leveraging of an Existing Authorization. The final approach, leveraged authorization, is employed when a DoD AO chooses to accept some or all of the information in an existing security authorization package generated by another federal agency or other DoD

Component (referred to in this instruction as the "owning organization") based on a need to use the same information resources (e.g., IS or services provided by the system). The DoD Component AO reviews the owning organization's security authorization package as the basis for determining risk to the leveraging organization before accepting the authorization. It is DoD policy that the reciprocal acceptance of existing DoD and other federal agency and department system authorizations (i.e., leveraged authorizations), and the artifacts contributing to the authorization decisions, must be employed to the maximum extent. See Enclosure 5 of this instruction and the KS for additional procedural guidance regarding reciprocity.

d. Security Plan. DoD IS and PIT systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

2. RMF STEPS. The RMF consists of the steps depicted in Figure 3. This process parallels the system life cycle, with the RMF activities being initiated at program or system inception (e.g., documented during capabilities identification or at the implementation of a major system modification). However, failure to initiate the RMF at system or program inception is not a justification for ignoring or not complying with the RMF. IS and PIT systems without ATOs must initiate the RMF in accordance with Enclosure 8 of this instruction and Tables 3 and 4, as appropriate, regardless of the system life-cycle stage (e.g., acquisition, operation). Chapter 3 of Reference (c) details the steps of the RMF, and paragraphs 2a through 2f provide amplifying DoD implementation guidance for those steps.

Figure 3. RMF for IS and PIT Systems



Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

a. Step 1 - Categorize System

(1) Categorize the system in accordance with Reference (e) and document the results in the security plan. Categorization of IS and PIT systems is a coordinated effort between the PM/SM, ISO, IO, mission owner(s), ISSM, AO, or their designated representatives. In the categorization process, the IO identifies the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. For acquisition programs, this categorization will be documented as a required capability in the initial capabilities document, the capability development document, the capabilities production document, and the cybersecurity strategy within the program protection plan (PPP). Specific guidance on determining the security category for information types and ISs is included in the KS.

(2) Describe the system (including system boundary) and document the description in the security plan.

(3) Register the system with the DoD Component Cybersecurity Program. See DoD Component implementing policy for detailed procedures for system registration.

(4) Assign qualified personnel to RMF roles. The members of the RMF Team are required to meet the suitability and fitness requirements established in DoD *Manual* 5200.02~~-R~~ (Reference (x)). RMF Team members must also meet appropriate qualification standards in

accordance with Reference (o). RMF team member assignments must be documented in the security plan.

(5) To avoid potential conflicts of interest or undue influence in RMF roles, certain designations or relationships will not be allowed. The AO or SCA cannot be or report to the PM/SM or program executive officer. The UR cannot be or report to the PM/SM.

b. Step 2 - Select Security Controls

(1) Common Control Identification. This task is the responsibility of the DoD CIO, DoD Component CIOs, and other organizations and entities that provide solutions for common controls. Common controls are selected as "common" and provided via the KS based on risk assessments conducted by these entities at the Tier 1 and Tier 2 levels. By identifying the security controls that are provided by the organization as common solutions for IS and PIT systems, and documenting the assessment and authorization of the controls in a security plan (or equivalent document), individual systems within those organizations can leverage these common controls through inheritance. See the KS for identification of common controls for DoD and additional information on how they are documented within the security authorization package.

(2) Security Control Baseline and Overlay Selection. Identify the security control baseline for the system, as provided in Reference (e), and document in the security plan. The baselines identified in Reference (e) address the overall threat environment for DoD IS and PIT systems. In this step, the applicable security controls baseline and relevant overlays for a system are assigned. See Reference (e) and the KS for detailed procedures. In brief, the process consists of:

(a) Selecting the applicable initial security control baseline from Reference (e) based on the IS categorization. These security control baselines identify the specific security controls from Reference (f) that are applicable to the system categorization.

(b) Identifying overlays that apply to the IS or PIT system due to information contained within the system or environment of operation. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security controls applicable to that system that is a combination of the baseline and overlay. The combination of baselines and overlays address the unique security protection needs associated with specific types of information or operational requirements. Overlays reduce the need for ad hoc or case-by-case tailoring by allowing COIs to develop standardized overlays that address their specific needs and scenarios. Access to the overlays, and guidance regarding how to determine which overlays may apply, are included in the KS. The KS is the authoritative source for detailed security control descriptions, implementation guidance and assessment procedures. Examples of overlays include:

1. Tactical environments.

2. PIT systems (including special categories of PIT systems, such as Industrial Control Systems or tactical PIT systems).

3. Personally identifiable information (PII) and Public Law 104-191, also known as the "Health Insurance Portability and Accountability Act" (Reference (y)), requirements.

4. Cross-domain requirements.

5. Classified information.

(c) If necessary, tailor (modify) a control set in response to increased risk from changes in threats or vulnerabilities, or variations in risk tolerance. The resultant set of security controls derived from tailoring is referred to as the tailored control set. Tailoring decisions must be aligned with operational considerations and the environment of the IS or PIT system and should be coordinated with mission owner(s) and URs. Security controls should be added or removed only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (e.g., mapping to risk tolerance) for those decisions, are documented in the security plan for the system. Every selected control must be accounted for either by the organization or the ISO or PM/SM. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the security plan and POA&M. The tailoring process may include:

1. Applying scoping guidance to the initial set of security controls;

2. Selecting or specifying compensating controls to adjust the initial set of security controls to obtain an equivalent set deemed to be more feasible to implement; or

3. Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored set of security controls.

(d) Supplementing the tailored baseline security control set, if necessary, with additional controls or control enhancements that consider local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances, and are based on risk assessments consistent with NIST SP 800-30 (Reference (j)).

(e) The resulting set of security controls is documented, along with the supporting rationale for selection decisions and any system use restrictions, in the security plan. The security plan must identify all common controls inherited from external providers, and establish minimum assurance requirements for those controls.

(3) Monitoring Strategy. Develop and document a system-level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation. The strategy must include the plan for annual assessments of a

subset of implemented security controls, and the level of independence required of the assessor (e.g., ISSM or SCA). The breadth, depth, and rigor of these annual assessments should be reflective of the security categorization of the system and threats to the system. The SCA should be integral to the development of this strategy. The system-level continuous monitoring strategy must conform to all applicable published DoD enterprise-level or DoD Component-level continuous monitoring strategies.

(4) Security Plan and System-Level Continuous Monitoring Strategy Review and Approval. The DoD Components will develop and implement processes whereby the AO (or designee) reviews and approves the security plan and system-level continuous monitoring strategy submitted by the ISO or PM/SM. By approving the security plan, the AO agrees to the system categorization, the set of security controls proposed to meet the security requirements for the system, and the adequacy of the system-level continuous monitoring strategy. The approval of the security plan also establishes the level of effort required to successfully complete the remainder of the steps in the RMF and provides the basis of the security specification for the acquisition of the system, subsystems, or components. For acquisition programs, approval should be accomplished before Milestone B and the issuance of the design and development request for proposals. If the security plan is deemed unacceptable, the AO or designated representative sends the plan back to the ISO or PM/SM for appropriate action. The AO approval of the security plan must be documented in the security plan.

c. Step 3 - Implement Security Controls

(1) Implement the security controls specified in the security plan in accordance with DoD implementation guidance found on the KS.

(a) Products used within an IS or PIT system boundary will be configured in accordance with applicable STIGs or SRGs where STIGs are not available.

(b) Security controls are implemented consistent with DoD and DoD Component ~~IA~~ *cybersecurity* architectures and standards, employing system and software engineering methodologies, security engineering principles, and secure coding techniques. DoD recommended security control implementation guidance is available on the KS.

(c) The ISO or PM/SM must ensure early and ongoing involvement by IS security engineers qualified in accordance with DoD 8570.01-M (Reference (z)). Mission owner(s) must translate security controls into system specifications, ensure the successful integration of those specifications into the system design, and ensure security engineering trades do not impact the ability of the system to meet the fundamental mission requirements. This includes ensuring that technical and performance requirements derived from the assigned security controls are included in requests for proposals and subsequent contract documents for design, development, production, and maintenance.

(d) The proposed system security design must be addressed in preliminary and critical design reviews. System security design should address security controls that may be inherited security controls, assessment test results and supporting documentation are maintained by the providing system and are made available to SCAs of receiving systems on request. For common controls inherited from the enterprise, instructions for documenting compliance are provided on the KS. SCAs will maximize the reuse of existing assessment (i.e., a leveraged authorization), and T&E documentation in their assessment of the system.

(a) Record Security Control Compliance Status. If no vulnerabilities are found through the process of executing the assessment procedures, the security control is recorded as compliant. If vulnerabilities are found, the control is recorded as NC in the POA&M, with sufficient explanation. Security controls that are not technically or procedurally relevant to the system, as determined by the AO, will be recorded as not applicable (NA) in the POA&M, with sufficient justification. The status and results of all security control assessments in the control set (see paragraph 2b(2) of this enclosure) will be recorded in the SAR. DoD implementation guidance and assessment procedures are available on the KS. Assessment procedures that are used that are not in accordance with the KS will be documented fully in the SAR.

(b) Assign Vulnerability Severity Value for Security Controls. Vulnerability severity values are assigned to all NC controls by the SCA as part of the security control analysis to indicate the severity associated with the identified vulnerability. Vulnerability severity values are identified in Reference (j). Vulnerability severity values for security controls are informed by assessment at the CCI level. If a control has a STIG or SRG associated through CCIs, the vulnerabilities identified by STIG or SRG assessments will be used to inform the overall vulnerability severity value for the security control.

(c) Determine Risk Level for Security Controls. The SCA determines and documents in the SAR a risk level for every NC security control in the system baseline. NC controls are subjected to a risk assessment process that considers multiple factors in producing the risk level. As described in Reference (j), these factors include, but are not limited to:

1. The SCA's determination that a credible or validated threat source and potential event exists that is capable of, and likely to, exploit vulnerabilities in the implementation of the control.

2. Vulnerability severity level and pre-disposing conditions. This includes the SCA's estimate of the adequacy of existing mitigations or compensating controls to address the vulnerability and mitigations provided by the hosting enclave, ~~CNDSP~~ *CSSP*, or other protective measures.

3. The cybersecurity attribute (i.e., confidentiality, integrity, or availability) and associated categorization impact level (high, moderate, low) related to the control.

4. The SCA's estimate of impact of a successful threat event.

(d) Assess and Characterize Aggregate Level of Risk to the System. The SCA must determine and document in the SAR an assessment of overall system level of risk (see levels of risk in Reference (j)), and identify the key drivers for the assessment. The SCA's risk assessment considers threats, vulnerabilities, and potential impacts as well as existing and planned risk mitigation. The risk assessment must address all NC controls, and clearly communicate the SCA's conclusion on system cybersecurity risk, and any recommendations for special instructions to accompany the authorization decision.

(3) Prepare the SAR, documenting the issues, findings, and recommendations from the security control assessment. The SAR documents the SCA's findings of compliance with assigned security controls based on actual assessment results. It addresses security controls in a NC status, including existing and planned mitigations. A SAR is always required before an authorization decision. If a compelling mission or business need requires the rapid introduction of a new IS or PIT system, assessment activity and a SAR are still required.

(4) Conduct remediation actions on NC security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate.

e. Step 5 - Authorize System

(1) Prepare the POA&M based on the vulnerabilities identified during the security control assessment. A full discussion and templates for preparing a POA&M is provided in the KS.

(a) A POA&M that the ISO or PM/SM develops:

1. Identifies tasks that need to be accomplished to remediate or mitigate vulnerabilities.

2. Specifies resources required to accomplish the elements of the plan.

3. Includes milestones for completing tasks and their scheduled completion dates.

(b) POA&Ms are maintained throughout the system life cycle. Once posted to the POA&M, vulnerabilities will be updated after correction or mitigation actions are completed, but not removed.

(c) Inherited vulnerabilities must be addressed on the POA&Ms. POA&Ms must be active throughout a system's life cycle as vulnerabilities remain or are remediated.

(d) The AOs, or AODRs, must monitor and track overall execution of POA&Ms under their responsibility.

(e) The ISO or PM/SM must implement the corrective actions identified in the POA&M. With the support and assistance of the ISSM, they must also provide visibility and status to the AO and the SISO.

(f) The DoD Component SISOs must monitor and track the overall execution of system-level POA&Ms across the entire Component until identified security vulnerabilities have been remediated and the RMF documentation is appropriately adjusted.

(2) Assemble the security authorization package and submit the package to the AO for adjudication. The ISSM assembles the security authorization package, consisting of the updated security plan, the SAR, and the POA&M. The security authorization package must also contain, or provide links to, the appropriate documentation for any security controls that are being satisfied through inheritance (e.g., security authorization packages, contract documents, MOAs, and SLAs). The security authorization package is submitted to the AO (via the AODR if appropriate) for review and final acceptance.

(3) Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The AO considers the current security state of the system (as reflected by the risk assessment and recommendations provided in the SAR), and weighs this against the operational need for the system. The AO must also consider any applicable risk-related guidance from the DoD SISO, PAOs, DoD ISRMC, DSAWG, DoD Component SISO, or mission owner(s). Weighing these factors, the AO renders a final determination of risk to DoD operations and assets, individuals, other organizations, and the Nation from the operation and use of the system. The KS provides additional guidance and tools for conducting system authorization risk assessments.

(4) Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The product of this risk determination is the authorization decision. An authorization decision applies to a specifically identified IS or PIT system and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DoD authorization decision is expressed as an ATO, an IATT, or a DATO. An IS or PIT system is considered unauthorized if an authorization decision has not been made.

(a) If overall risk is determined to be acceptable, and there are no NC controls with a level of risk of "Very High" or "High," then the authorization decision should be issued in the form of an ATO. An ATO authorization decision must specify an ATD that is within 3 years of the authorization date unless the IS or PIT system has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued.

(b) If NC controls with a level of risk of "Very High" or "High" exist that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision will be issued in the form of an ATO with conditions and only with permission of the responsible DoD Component CIO. If the system still requires operation with a level of risk of "Very High" or "High" after 1 year, the DoD Component CIO must again grant permission for continued operation of the system. This authority cannot be delegated below the DoD Component CIO. The DoD Component CIO must concur in writing or through DoD public key infrastructure (PKI)-certified digital signature that the security risk of continued system operation is acceptable due to mission criticality. The DoD Component CIO provides a copy of the concurrence and authorization decision document with supporting rationale to the DoD ISRMC Secretariat and the DoD SISO. This authorization decision closely manages risk while allowing system operation. The ATOs with conditions should specify an AO review period that is within 6 months of the authorization date. The POA&M supporting this ATO documents identified vulnerabilities and specifies corrective actions to be completed before the review.

(c) If the risk determination is being made to permit testing of the system in an operational information environment or with live data, and the risk is acceptable, then the authorization decision should be issued in the form of an IATT.

1. IATTs should be granted only when an operational environment or live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical), and should expire at the completion of testing (normally for a period of less than 90 days). Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period). The application of an IATT in support of DT&E needs to be planned, resourced, and documented within the program T&E plan in accordance with Reference (r).

2. For full and independent operational testing, an ATO (rather than an IATT) may be required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities. In this case, the ATO should be reviewed following operational testing and evaluation for modification as necessary in consideration of the operational test results.

3. All applicable security controls should be tested and satisfied before testing in an operational environment or with live data except for those that can only be tested in an operational environment. In consultation with the ISO or PM/SM, the AO will determine which security controls can only be tested in an operational environment.

(d) If risk is determined to be unacceptable, the authorization decision should be issued in the form of a DATO. If the system is already operational, the AO will issue a DATO and stop operation of the system immediately. Network connections will be immediately terminated for any system issued a DATO. A DATO may also be issued coincidental to implementing a decommissioning strategy for a system.

(e) Documentation supporting an authorization decision will be provided in electronic form if requested by AOs of interconnecting IS and PIT systems.

f. Step 6 - Monitor Security Controls

(1) Determine the security impact of proposed or actual changes to the IS or PIT system and its environment of operation. Included in the security controls assigned to all IS and PIT systems are security controls related to configuration and deficiency management, performance monitoring, and periodic independent evaluations (e.g., penetration testing).

(a) The ISSM, in coordination with other appropriate personnel (e.g., IS security engineer, system administrators, ~~CNDSP~~ *CSSP*):

1. Continuously monitors the system or information environment for security-relevant events and configuration changes that negatively affect security posture.

2. Periodically assesses the quality of security controls implementation against performance indicators, such as: security incidents; feedback from external inspection agencies (e.g., OIG DoD, Government Accountability Office (GAO)); exercises; and operational evaluations, including Director, OT&E ~~IA,~~ assessments.

3. Must report any significant change in the security posture of the system, and recommended mitigations, immediately to the SCA and AO.

4. May recommend to the SCA or AO a reassessment of any or all security controls at any time.

(2) Assess a subset of the security controls employed within and inherited by the IS or PIT system in accordance with the AO-approved system-level continuous monitoring strategy.

(a) The assessor must provide a written and signed (or if digital, DoD PKI-certified digitally signed) report in the SAR format to the AO that indicates the results of an annual assessment of selected security controls. Reference (c) provides additional guidance on conducting annual assessments.

(b) The results of the annual assessment must be documented in an SAR, which will recommend either no change to the authorization status or downgrade to a DATO. The POA&M will also be updated as appropriate.

(c) The AO must review the SAR in light of mission and information environment indicators and determine a course of action that will be provided to the responsible CIO or SISO for reporting requirements described in FISMA. An AO may downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant.

(3) Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M. Systems with a current ATO that are found to be operating in an unacceptable cybersecurity posture through Director, OT&E ~~IA,~~ assessments, GAO audits, OIG DoD audits, or other reviews or events (such as an annual security review or compliance assessment) must have the newly identified vulnerabilities and associated level of risk added to an existing or newly created POA&M.

(4) The PM/SM ensures the security plan and POA&M are updated based on the results of the system-level continuous monitoring process. The ISSM may recommend changes or improvement to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system itself to the SCA and AO at any time.

(5) Report the security status of the system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

(6) The AO reviews the reported security status of the system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation remains acceptable.

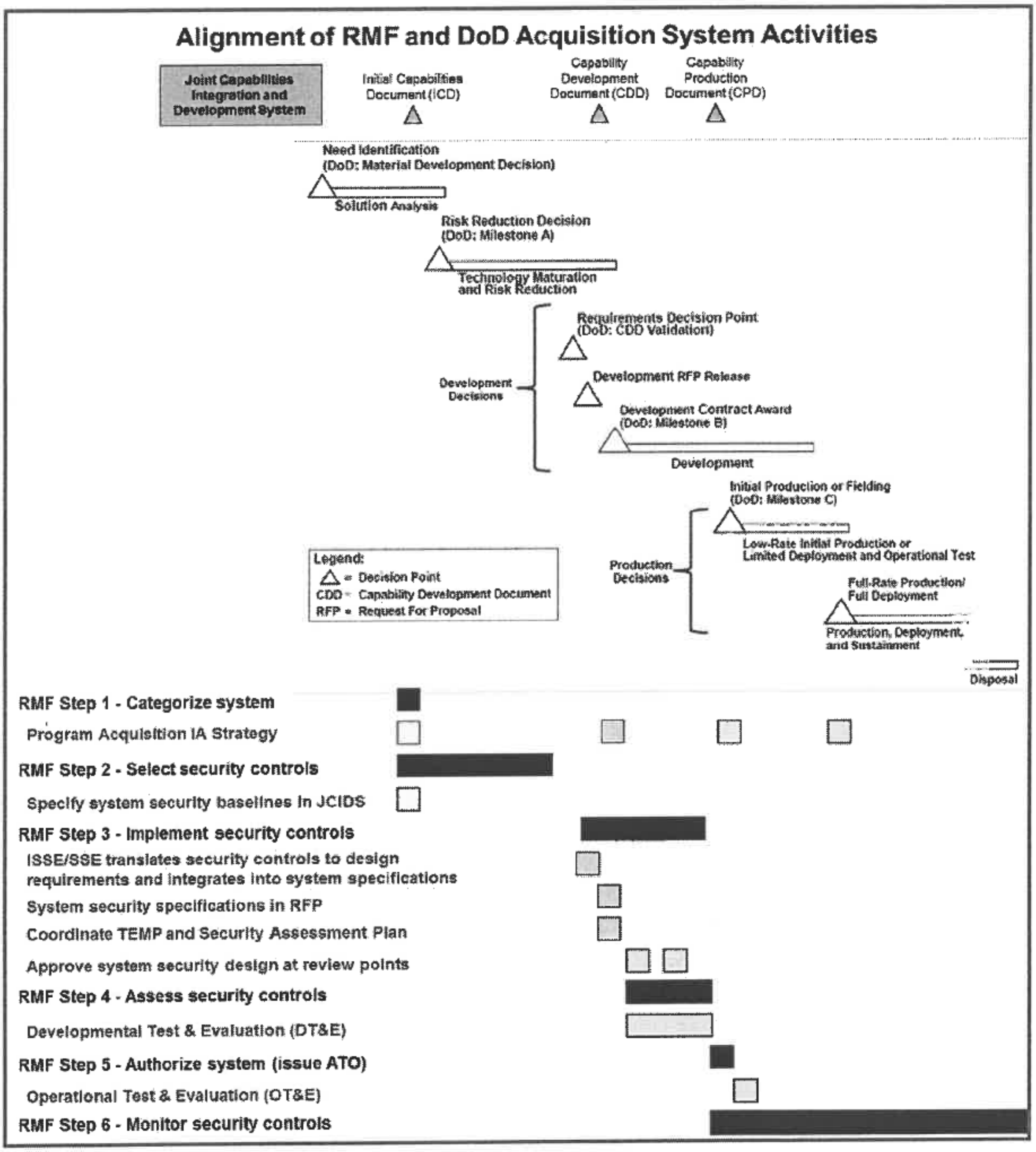
(a) In accordance with Appendix III to OMB Circular A-130 (Reference (aa)), systems must be reassessed and reauthorized once every 3 years. The results of an annual review or a major change in the cybersecurity posture at any time may also indicate the need for reassessment and reauthorization of the system.

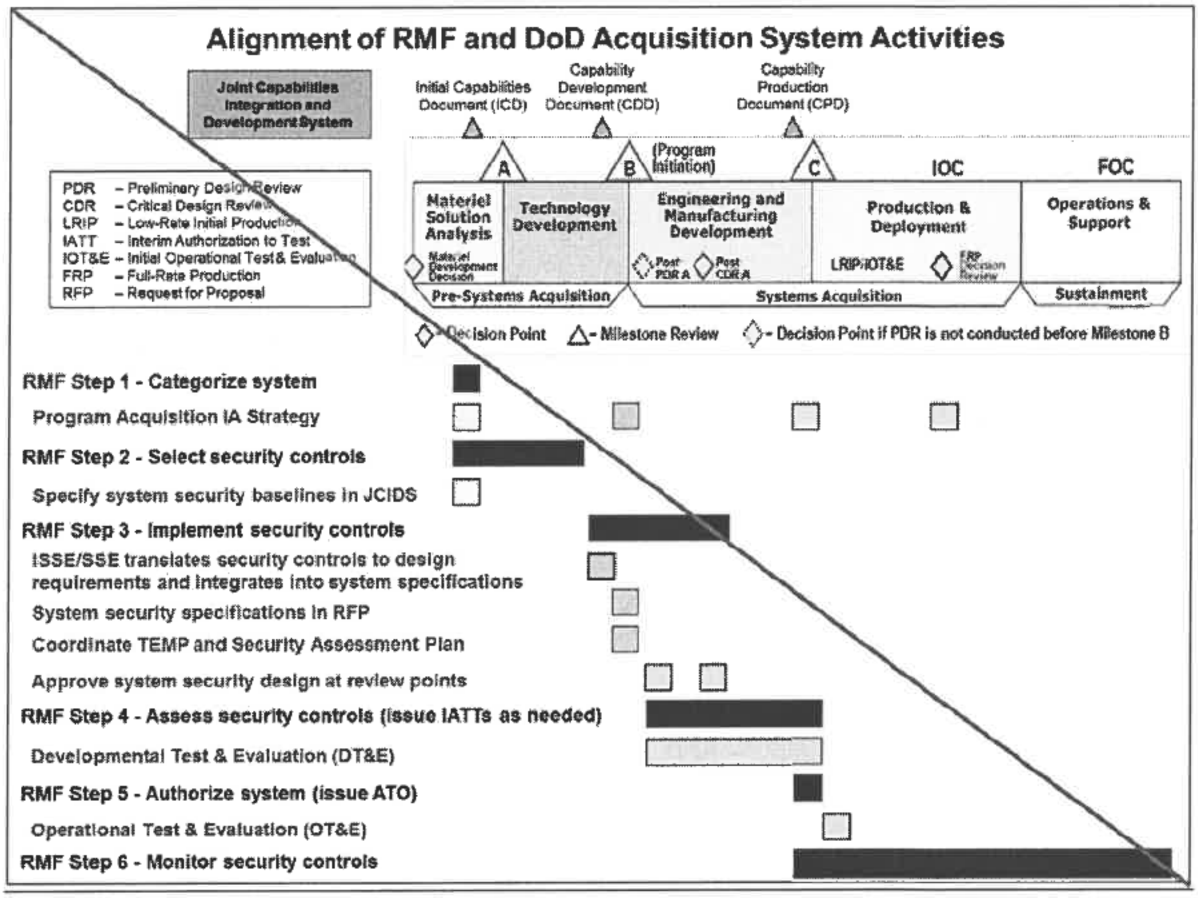
(b) Systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program (as defined by emerging DoD continuous monitoring policy) may operate under a continuous reauthorization. Continuous monitoring does not replace the security authorization requirement; rather, it is an enabler of ongoing authorization decisions.

(7) Implement a system decommissioning strategy, when needed, which executes required actions when an IS or PIT system is removed from service. When a system is removed from operation, a number of RMF-related actions are required. Before decommissioning, any control inheritance relationships should be reviewed and assessed for impact. Once the system has been decommissioned, the security plan should be updated to reflect the system's decommissioned status, and the system should be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in cybersecurity infrastructures that support the DoD Information Enterprise, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact.

3. INTEGRATING THE RMF INTO THE DEFENSE ACQUISITION MANAGEMENT SYSTEM. The RMF is designed to be complementary to and supportive of DoD's acquisition management system activities, milestones, and phases. RMF activities should be initiated as early as possible in the DoD acquisition process to increase security and decrease cost. Requirements development, procurement, and T&E processes should be considered in applying the RMF to the acquisition of DoD IT. Threats to these systems should be designated consistent with the most severe risk to any individual component or subcomponent for consideration of requirements, acquisition, and testing and evaluation. Figure 4 illustrates the alignment of RMF steps to the acquisition life cycle.

Figure 4. RMF and the Defense Acquisition Management System


Alignment of RMF and DoD Acquisition System Activities
Joint Capabilities Integration and Development System
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
Need Identification
(DoD: Material Development Decision)
Solution Analysis
Risk Reduction Decision
(DoD: Milestone A)
Technology Maturation and Risk Reduction
Requirements Decision Point
(DoD: CDD Validation)
Development Decisions
Development RFP Release
Development Contract Award
(DoD: Milestone B)
Development
Initial Production or Fielding
(DoD: Milestone C)
Low-Rate Initial Production or Limited Deployment and Operational Test
Production Decisions
Full-Rate Production/ Full Deployment
Production, Deployment, and Sustainment
Disposal
Legend:
△ = Decision Point
CDD = Capability Development Document
RFP = Request For Proposal
RMF Step 1 - Categorize system
Program Acquisition IA Strategy
RMF Step 2 - Select security controls
Specify system security baselines in JCIDS
RMF Step 3 - Implement security controls
ISSE/SSE translates security controls to design requirements and integrates into system specifications
System security specifications in RFP
Coordinate TEMP and Security Assessment Plan
Approve system security design at review points
RMF Step 4 - Assess security controls
Developmental Test & Evaluation (DT&E)
RMF Step 5 - Authorize system (issue ATO)
Operational Test & Evaluation (OT&E)
RMF Step 6 - Monitor security controls



Alignment of RMF and DoD Acquisition System Activities

Joint Capabilities Integration and Development System
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
A
B
(Program Initiation)
C
IOC
FOC
PDR – Preliminary Design Review
CDR – Critical Design Review
LRIP – Low-Rate Initial Production
IATT – Interim Authorization to Test
IOT&E – Initial Operational Test & Evaluation
FRP – Full-Rate Production
RFP – Request for Proposal
Materiel Solution Analysis
Materiel Development Decision
Technology Development
Engineering and Manufacturing Development
Post PDR A
Post CDR A
Production & Deployment
LRIP/IOT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
◇- Decision Point
△- Milestone Review
◇- Decision Point if PDR is not conducted before Milestone B
RMF Step 1 - Categorize system
Program Acquisition IA Strategy
RMF Step 2 - Select security controls
Specify system security baselines in JCIDS
RMF Step 3 - Implement security controls
ISSE/SSE translates security controls to design requirements and integrates into system specifications
System security specifications in RFP
Coordinate TEMP and Security Assessment Plan
Approve system security design at review points
RMF Step 4 - Assess security controls (issue IATTs as needed)
Developmental Test & Evaluation (DT&E)
RMF Step 5 - Authorize system (issue ATO)
Operational Test & Evaluation (OT&E)
RMF Step 6 - Monitor security controls

4. SECURITY AUTHORIZATION DOCUMENTATION. The security authorization documentation consists of all artifacts developed through RMF activity. Security authorization documentation is maintained throughout a system's life cycle. The security authorization package consists of the security plan, SAR, POA&M, risk assessment report, authorization decision document, and is the minimum information necessary for the acceptance of an IS or PIT system by a receiving organization. Detailed information on the content of the security authorization package is available on the KS.

ENCLOSURE 8

RMF TRANSITION

1. DoD IS and PIT systems will transition to the RMF in accordance with Table 2. All IS and PIT systems must transition to the Reference (e) categorization and security controls selection methodology, Reference (f) security control catalog, and the RMF.

2. Components are authorized and encouraged to start using RMF immediately. Recognizing the transition to RMF is complex; Table 2 establishes the timeline for the authorized continued use of DIACAP.

3. There are three key events in Table 2:

a. The date the package is submitted to the AO; this date determines the maximum duration of the ATO.

b. The date the package is signed by the AO (i.e. ATO date); this date starts the clock on the ATO.

c. The ATD, based on the maximum duration of the ATO, is calculated from the AO signature date/ATO Date.

4. Table 2 provides a staggered timeline, and ATO duration for IS and PIT systems under the DIACAP. The timelines apply to new system authorizations as well as existing systems with an expiring ATO. All IS and PIT systems must comply.

5. In the case of significant financial or operational impacts of transitioning to RMF, an AO may submit a request for deviation from this guidance for specific systems to the respective DoD Component CIO for approval. All requests for deviation forwarded to the Component CIO must be accompanied by an IS transition plan and a plan of action and milestones.

Table 2. RMF Initial Transition Timeline and Instructions

Completed DIACAP Package Submitted to AO for Signature	ATO Date	Maximum Duration of ATO under DIACAP
Signature date of this document through May 31, 2015	Determined by AO Signature Date	2.5 years from AO signature date
June 1, 2015 through February 1, 2016		2 years from AO signature date
February 2, 2016 through October 1, 2016		1.5 years from AO signature date

6. Transition to updated versions of Reference (e) will be in accordance with Table 3 for IS and PIT systems that have transitioned to the RMF.

Table 3. Transition Timeline and Instructions – Updates to CNSSI 1253

DoD System Authorization Status		Transition Timeline and Instructions (Upon publication of future versions of CNSSI 1253)
1	New start or unauthorized operational system (No initiated RMF activity or Component PIT system certification and accreditation activity).	Transition to new versions of CNSSI 1253 within 6 months of publication of updates and execute RMF.
2	System has initiated RMF, but has not yet begun executing the security plan.	Transition to new versions of CNSSI 1253 within 6 months of publication of updates and execute RMF.
3	System has begun executing the RMF security plan.	Either: a. Continue under the current version of CNSSI 1253. Develop a strategy and schedule for transitioning to the new version of CNSSI 1253. Obtain AO's approval of the strategy and schedule. The schedule for transitioning must not exceed the system re-authorization timeline. Or; b. Transition to the new version of CNSSI 1253 and execute RMF.
4	System has an RMF or equivalent DoD Component PIT system authorization decision that is current within 3 years.	Develop a strategy and schedule for transitioning to the new version of CNSSI 1253. Obtain AO's approval of the strategy and schedule. The schedule for transitioning must not exceed the system re-authorization timeline.
5	System has an RMF or equivalent DoD Component PIT system authorization that is more than 3 years old.	Transition to the new version of CNSSI 1253 immediately and execute RMF.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	authorizing official
AODR	authorizing official designated representative
ATD	authorization termination date
ATO	authorization to operate
BMA	business mission area
CAC	common access card
CCI	control correlation identifier
CDS	cross domain solution
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
~~CNDSP~~ *CSSP*	~~computer network defense~~ *cybersecurity* service provider
CNSSI	Committee on National Security Systems Instruction
COI	community of interest
DASD(DT&E)	Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
DATO	denial of authorization to operate
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIMA	DoD portion of the intelligence mission area
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	DoD Chief Information Officer
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	DoD Directive
DoDI	DoD Instruction
DOT&E	Director, Operational Test and Evaluation
DSAWG	Defense ~~IA~~-Security *Cybersecurity* ~~Accreditation~~ *Authorization* Working Group
DT&E	developmental test and evaluation
EIEMA	enterprise information environment mission area
eMASS	Enterprise Mission Assurance Support Service
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
~~GIG~~	~~Global Information Grid~~

IA	information assurance
IATT	interim authorization to test
IO	information owner
IS	information system
ISO	information system owner
ISRMC	Information Security Risk Management Committee
ISSM	information system security manager
ISSO	information system security officer
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
KS	Knowledge Service
MA	mission area
MOA	memorandum of agreement
MOU	memorandum of understanding
NA	not applicable
NC	non-compliant
NIST	National Institute of Standards and Technology
OIG DoD	Office of the Inspector General of the Department of Defense
OMB	Office of Management and Budget
OT&E	operational test and evaluation
PAO	principal authorizing official
PII	personally identifiable information
PIT	platform information technology
PKI	public key infrastructure
PM	program manager
PM/SM	program manager/system manager
POA&M	plan of action and milestones
PPP	program protection plan
RMF	risk management framework
SAR	security assessment report
SCA	security control assessor
SCI	sensitive compartmented information
SISO	senior information security officer
SLA	service level agreement
SM	system manager
SP	Special Publication
SRG	security requirements guide
STIG	security technical implementation guide

TAG	Technical Advisory Group
T&E	test and evaluation
UC	unified capabilities
UR	user representative
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USSTRATCOM	United States Strategic Command
WMA	warfighting mission area

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

application. Defined in CNSSI 4009 (Reference (ab)).

authorization. Defined in Reference (c).

authorization boundary. Defined in Reference (c).

AO. Defined in Reference (ab).

AODR. An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization

ATO. Defined in Reference (ab).

CCI. Defined in Reference (h).

CDS. Defined in Reference (ab).

common controls. Defined in Reference (c).

cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (ac)).

DoD Information Enterprise. Defined in DoDD 8000.01 (Reference (k)).

DoD IT. Defined in Reference (h).

enclave. Defined in Reference (ab).

hardware. Defined in Reference (ab).

IATT. Defined in Reference (ab).

IT product. Defined in Reference (h).

IT Service. Defined in Reference (h).

IO. Defined in Reference (ab).

IS. Defined in Reference (ab).

ISO. Defined in Reference (c), but for the purposes of this instruction is not synonymous with "PM" as indicated in Reference (c).

ISSM. Defined in Reference (ab).

ISSO. Defined in Reference (ab).

MA. Defined in Reference (m).

Milestone B. Defined in Reference (r).

mission partners. Defined in Reference (k).

network. Defined in Reference (ab).

penetration testing. Defined in Reference (ab).

PIT. Defined in Reference (h).

PIT system. Defined in Reference (h).

PM/SM. Defined in Reference (h).

POA&M. Defined in Reference (ab).

reciprocity. Defined in Reference (ab).

risk. Defined in Reference (ab).

risk assessment. Defined in Reference (ab).

risk executive function. Defined in Reference (ab).

risk management. Defined in Reference (ab).

risk mitigation. Defined in Reference (ab).

RMF. Defined in Reference (ab).

SAR. Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.

SCA. Defined in Reference (c).

SCI. Defined in Reference (ab).

security. Defined in Reference (ab).

security assessment plan. Provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. See Reference (g) for additional information regarding security assessment plans.

security control assessment. Defined in Reference (ab).

security control baseline. Defined in Reference (ab).

security controls. Defined in Reference (ab).

security domain. Defined in Reference (ab).

security plan. Defined in Reference (c).

SLA. Defined in Reference (ab).

software. Defined in Reference (ab).

SRG. Defined in Reference (h).

STIG. Defined in Reference (h).

type authorization. A method of system authorization that allows a single security authorization package to be developed for an archetype (common) version of a system, and the issuance of a single authorization decision that is applicable to multiple deployed instances of the system.

UC. Defined in Reference (v).

UR. Defined in Reference (ab).

TAB Q

DEPARTMENT OF THE ARMY
UNITED STATES ARMY NETWORK ENTERPRISE TECHNOGLOGY COMMAND
GREELY HALL, 2133 CUSHING STREET
FORT HUACHUCA, ARIZONA 85613-7070

NETC-CS 26 March 2020

MEMORANDUM THRU Commander, 7th Signal Command (Theater), 423 22nd Street, Building 21715, Fort Gordon, GA 30905-5832

MEMORANDUM FOR Commander, 21st Signal Brigade, 1435 Porter Street, Fort Detrick, Maryland 21702-5046

SUBJECT: Approval of Report of Investigation for Whistleblower Investigation Concerning Office of Special Counsel Referral DI-17-2168, Department of the Army, 1st Personnel Command, Washington-Moscow Direct Communications Link, Detrick Earth Station, Fort Detrick, Maryland

1. The findings and recommendations of the Report of Investigation (ROI) for Whistleblower Investigation Concerning Office of Special Counsel Referral DI-17-2168, Department of the Army, 1st Personnel Command, Washington-Moscow Direct Communications Link, Detrick Earth Station, Fort Detrick, Maryland, are approved.

2. The enclosed ROI is forwarded from the undersigned as the Appointing Authority, through Commander, 7th Signal Command (Theater), to the Commander, 21st Signal Brigade for appropriate action consistent with the findings. Specifically, the Commander, 21st Signal Brigade will:

a. Complete the Configuration Control Board (CCB) charter that was initiated by a previous 21st Signal Brigade Commander.

b. Staff a memorandum through 7th Command, NETCOM, and ARCYBER, to CIO/G-6 requesting that the CIO/G-6 chair the CCB in accordance with Army regulation.

c. Request Fort Detrick Fire Marshal conduct an inspection of the building.

d. Initiate the risk management process requirements at Detrick Earth Station in accordance with the new risk management framework.

3. The Commander, 21st Signal Brigade has 30 days from the date of this memorandum to implement the actions above and to report to me on any other action taken to comply with the findings and recommendations documented in the ROI.

Encl

[redacted]
COL, GS
Chief of Staff

TAB R

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC 3 Apr 20

[redacted] Digitally signed by [redacted]
MON.1105982808 808
Date: 2020.04.07 16:21:26 -04'00'

MEMORANDUM THRU Commanding General (NETC-SFC-CG), 7th Signal Command (Theater), 423 22nd Street, Building 21715, Fort Gordon, GA 30905-5832

FOR Commanding General (NETC-CG), Network Enterprise Technology (NETCOM), 2133 Cushing Street, Fort Huachuca, AZ 85613

SUBJECT: Implementation of Findings for Direct Communications Link (DCL) Detrick Earth Station (DES)

1. Reference Memorandum, Network Enterprise Technology Command (NETCOM), NETC-CS, 26 Mar 20, subject: Approval of Report of Investigation for Whistleblower Investigation Concerning Office of Special Counsel Referral DI-17-2168, Department of the Army, 1st Personnel Command, Washington-Moscow Direct Communications Link, Detrick Earth Station, Fort Detrick, Maryland.

2. This memorandum provides a response and timeline for the items listed in par. 2 of the reference.

3. Detailed responses:

a. "*Complete the Configuration Control Board (CCB) charter that was initiated by a previous 21st Signal Brigade Commander.*" Completed, see enclosure 1. The charter draft is prepared for review upon the initiation of the CCB of item 3b below.

b. "*Staff a memorandum through 7th Command, NETCOM, and ARCYBER, to CIO/G-6 requesting that the CIO/G-6 chair the CCB in accordance with Army regulation.*" Completed, see enclosure 2. The memorandum, NETC-SYD, 3 Apr 20, subject: Direct Communications Link (DCL) Configuration Control Board (CCB) is routing.

c. "*Request Fort Detrick Fire Marshal conduct an inspection of the building.*" Completed, see enclosure 3. The request of the Fort Detrick Fire Marshal was made on 2 APR 20. The inspection is scheduled for 6 Apr 20.

d. "*Initiate the risk management process requirements at Detrick Earth Station in accordance with the new risk management framework.*" Completed, see enclosure 4. Mr [redacted] Chief, Senior National Leadership Communications Division (OPC/IE/IE8), DISA, provided the document at enclosure 4 (DISA Form 9, 25 Feb 20, subject: DCL AO Approval for NSA Network Assessment). It is his determination that Mr. [redacted], Sr., SES, RME/RE/CIO, Risk Management Executive/

Authorizing Official, of DISA is the Authorizing Official (AO). [redacted] submission shows the initiation of the accreditation of the DCL/DES within the DISA AO's purview.

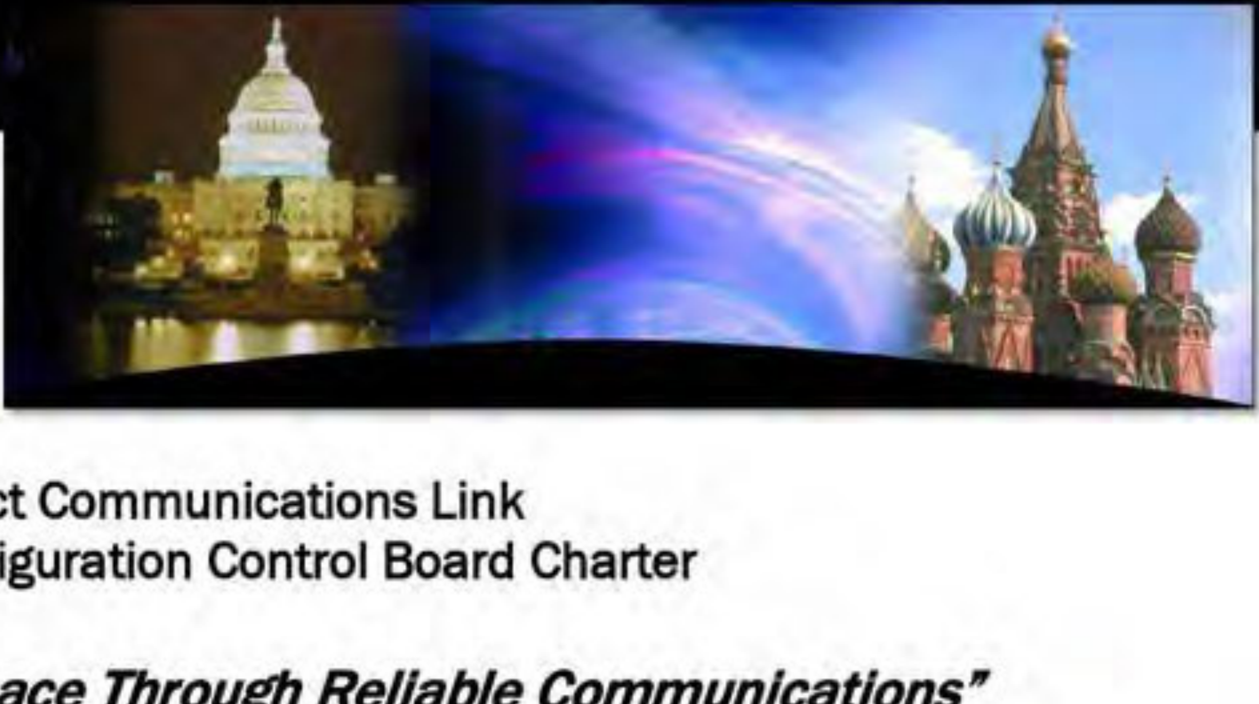
4. Team 21 - "Edge of the Sword."

[redacted] Digitally signed by
[redacted]
Date: 2020.04.03 19:39:08 -04'00'

[redacted]
COL, SC
Commanding

4 Encls
1. Draft CCB Charter
2. CCB Restart Memo, 3 Apr 20
3. Fire Marshall Memo, 2 Apr 20
4. DISA Form 9, 25 Feb 20

Department of the Army
CIO/G-6



Direct Communications Link Configuration Control Board Charter

"Peace Through Reliable Communications"

May 2020

Table of Contents

Charter, Direct Communications Link Configuration Control Board

1.0 Authorities, Objectives and Scope

The Direct Communications Link (DCL) Configuration Control Board (CCB) is chartered through the Army Chief Information Officer (CIO)/G-6 to successfully identify engineering plans, configuration standards and designs, and implementations that support operational requirements for the DCL. The CCB will work to ensure interoperability and synchronization between all stakeholders.

This charter establishes the Army DCL CCB and assigns responsibilities for establishing and maintaining of technical and functional baselines for the system. The Army DCL CCB will operate in an integrated and disciplined manner to provide a structured and streamlined control process for managing the assigned products and services throughout their intended life cycle. Life cycle configuration management through the CCB ensures that all changes are visible, that any potential safety, security and operational impacts are properly addressed, and that technical and programmatic direction across the DCL system's products, services and interfaces are consistent.

1.1 Authorities

1.1.1 USD C4I

Under Secretary of Defense for Command, Control, Communications and Intelligence Memorandum Subject: Upgrade to the US/USSR Direct Communications Link (DCL) dated 14 March 1984 designated the Army as Lead Military Department for the DCL.

1.1.2 NSD-301

National Security Directive – 301 (NSD-301), dated February 1988, assigned life cycle support responsibility, on a reimbursable basis, to the Department of the Army for the Nuclear Risk Reduction Center (NRRC) program.

1.1.3 ASD C41

Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandum Subject: Designation of Army as Lead Military Department (LMD) for the Direct Communications Link (DCL), the Continuous Communications Link (CCL) and the Government to Government Communications Links (GGCLs) dated 28 July 2000 reaffirmed the Army's designation as LMD for the DCL, CCL and GGCLs.

1.1.4 ASD NII

Assistant Secretary of Defense for Networks and Information Integrations / DoD Chief Information Officer (ASD(NII)/DoD CIO) Memorandum Subject: Communications With Other Nations (CWON) dated 28 April 2009 established the National Leadership

Command Capability (NLCC) Executive Management Board (EMB) to coordinate CWON issues.

1.1.5 DODD 8000.01

Department of Defense Directive 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), dated 27 July 2017.

1.1.6 AR 25-1

Army Regulation 25-1 Information Management, Army Information Technology, dated 15 July 2019.

1.2 Objectives

- Serve as the focal point for Direct Communications Link activities
- Review, coordinate, synchronize and approve system changes
- Ensure Direct Communications Link cyber compliance
- Promote the efficient operation of cross-functional and cross-organizational business processes

1.3 Scope

The DLC CCB operates under the authority and in support of the Army Chief Information Officer/G-6 (CIO/G-6) and the Defense Information Systems Agency (DISA) for support of Communications With Other Nations (CWON) Systems. The approving authority for the CCB Charter is the Army CIO/G-6. The CCB determines DCL future capability development and prioritizes, approves, plans and integrates requests for change into the current and future systems throughout the life cycle and ensures all efforts are coordinated with the National Leadership Command Capability (NLCC) Executive Management Board (EMB). The CCB represents the interests of all stakeholders of the DCL systems and/or may be affected by changes to the DCL configuration item (CI) baselines.

The scope of the CCB activities include:

- IT engineering in support of the DCL
- Review and evaluation of proposed DCL lifecycle upgrades and design solutions
- Activities and engineering related to Cyber, NetOps, networks, operations management and defense of the DCL systems and services
- Development, oversight and maintenance of policies, standards and procedures for the use of the DCL
- Determination of whether projects and plans align and comply with the published IT standards and policies
- Determination to include or exclude new technologies and services into the DCL infrastructure

- Support the development and management of DCL technical architecture blueprints and standards
- Architecture technical compliance reviews
- Recommendations to the Enterprise Authorizing Official

2.0 Membership

The DCL CCB is comprised of voting members and non-voting members. Voting members represent the community's interests in the following areas; Policy; Planning, Programming and Budget; Technical and Engineering; Operations and Maintenance. Non-voting members of the CCB represent the other Federal Agencies and User Communities that provide information and assistance to the CCB. The Director, Networks, Systems & Services Directorate, Army CIO/G-6 has been designated as the CCB Chair. The DISA Communications With Other Nations (CWON) Program Manager is designated as the CCB Deputy Chair. Voting members must be empowered by their organizations, by memorandum, with the authority to make decisions on all matters coming before the CCB.

All voting members of the CCB are expected to be present for all CCB meetings. Geographically dispersed members may participated by video teleconference or telephone. Voting members, with the prior approval of the CCB Chair, may designate, by memorandum, an alternate representative in those instances when the primary representative is not available. A quorum necessary for conducting CCB functions is reached when 80% of the voting members are represented at the meeting.

2.1 Chair

Director, Networks, Services & Strategy, Directorate, CIO/G-6.

2.2 Deputy

Program Manager, Communications With Other Nations (CWON), DISA.

2.3 Secretary

Civilian Deputy to the Commander, 21st Signal Brigade, Fort Detrick, Maryland.

2.4 Membership

2.4.1 Voting Members

Representatives for the following agencies/organizations constitute the voting members of the DCL CCB.

- Army CIO/G-6, Director, Networks, Services & Strategy, Directorate, CIO/G-6, CCB Chair

- Program Manager, Communications With Other Nations (CWON), DISA, Deputy Chair
- Civilian Deputy to the Commander, 21st Signal Brigade, Secretary
- Army Project Manager Defense Communications and Army Transmission System (PM DCATS), CCB Member, Programming and Budget
- Army Information Systems Engineering Command (ISEC), CCB Member, Technical and Engineering
- Army Network Enterprise Technology Command (NETCOM) Assistant Chief of Staff (ACofS) G-3/5/7, CCB Member, Operations and Maintenance

2.4.2 Non-voting Members

All non-voting members may participate in the CCB at their discretion. Information presented by the non-voting members will be considered by the CCB prior to final decisions.

Representatives from the following agencies/organizations constitute the non-voting members of the DCL CCB.

- Chief, Washington-Moscow Direct Communications Link (MOLINK), J3, Joint Staff
- Staff Director, Department of State Bureau of Arms Control, Verification, and Compliance (AVC) Nuclear Risk Reduction Center (NRRC)
- NRRC Branch, Department of State Information Resource Management (IRM)
- Telecommunications Division, DISA White House Communications Agency (WHCA)
- Information Assurance Manager, CWON, DISA

3.0 Duties of the Board Members

3.1 The Chair

- Direct all CCB activities
- Call and chair (i.e., lead) CCB meetings
- Assign actions and tasks
- Establish subordinate tiger teams and integrated process teams (IPTs) as needed
- Approve agendas and minutes
- Ensure dissemination and coordination of information to all appropriate stakeholders
- Identify, prioritize and approve initiatives and decisions for submission to the CCB
- Resolve other issues as required

3.2 The Deputy

- Support the Chair and act as the Chair in his absence

- Coordinate and synchronize member activities in support of the objectives and scope of the CCB
- Be the initial focal point for resolution of engineering related issues that arise
- Provide advice and counsel to the Chair on Board matters
- Disseminate specific requirements for data and other actions on behalf of the Board
- Structure issues and ensure proper representation on items before the Board
- Monitor and track follow-on actions taken to ensure that decisions reached and assignments made by the Board Chair/Board are implemented properly
- Support and coordinate the activities of the Board's subordinate bodies

3.3 The Secretary

- Publish agendas, coordinate and schedule meetings at the Chair's direction
- Facilitate the Chair and Deputy to coordinate activities during actual meetings
- Develop and publish the official minutes, resolutions and actions of the CCB
- Ensure all security rules and regulations regarding classified meetings and documents are followed
- Assemble, prepare and distribute material on matters under consideration by the Board at least three working days in advance
- Maintain collaboration sites, minutes, agendas, wikis, blogs and knowledge centers
- Compile and maintain contact lists for the Board members, their coordinating staffs and any subordinate bodies

3.4 CCB Members

- Represent organizational positions on CCB issues
- Sponsor items and issues for meetings, including preparation of position papers, read-ahead materials and presentation of briefings
- Identify and nominate agenda items and issues to the Chair for consideration
- Ensure dissemination and coordination of CCB information to all appropriate organizational stakeholders and staffs working source material (e.g., technical documents) as necessary to ensure open collaboration
- Convey and support CCB positions and decisions to their organizations
- Execute actions and tasks as directed by the Chair
- Ensure member organizations are represented on appropriate CCB subordinate bodies, e.g., Tiger Teams
- Designate an alternate CCB representative responsible for attending meetings in the absence of the principal representative
- Designate members and subject matter experts for standing and ad-hoc working groups
- Review minutes

4.0 Subordinate Bodies

Tiger Teams and IPTs are organized and participate as needed within the CCB.

The Purpose of the Tiger Team/IPT is to act as an SME group to facilitate senior level decision-making to this end:

1. Provide advice to the CCB to help make presentations more concise, accurate and understandable.

2. Identify potential conflicts and work to obtain resolution at the lowest level.

3. Champion CCB issues and positions within military organizations to gain working level support.

4. Disseminate CCB information to all appropriate organizational stakeholders and staffs working documents as necessary to ensure open collaboration.

Tiger Teams/IPTs report to the CCB. IPTs will be formed for efforts that are considered "longer term" in nature, e.g., for efforts that are expected to last 6 months or longer. The CCB will direct the creation of IPTs. The CCB will designate the leads and membership of the IPT, following the guidance given by the CCB.

Tiger Teams will be formed for efforts that are considered "shorter term" in nature, e.g., for efforts that are expected to last less than 6 months. Tiger Teams will normally support and report to IPT leads.

5.0 Operating Procedures

5.1 Leadership

The DCL CCB will meet quarterly or at the call of the CCB Chair. The DCL CCB will establish a configuration management (CM) plan that documents all CM roles, responsibilities and procedures for implementation of CCB approved Engineering Requests (ERs) and Engineering Change Proposals (ECPs).

The CCB Chair, with support from the CCB secretary, will:

- Establish and maintain the DCL CCB portal site that will be used to disseminate and collect CCB information and data.
- Schedule CCB meetings and locations.
- Publish meeting agendas.
- Provide advance status on ERs, ECPs, Schedule Releases, and Independent Verification and Validation (IV&V) activities and other items to be addressed by the CCB no later than three weeks prior to a scheduled CCB meeting.

- Request CCB voting members review the advance information and formulate a vote on CCB Chair recommendations that are not anticipated to be controversial.
- Conduct CCB meetings and record meeting minutes to include an annotated list of ERs and ECPs as approved, rejected, or deferred.
- Approved ERs and ECPs will be scheduled for implementation as part of the overall DCL schedule. Deferred ERs and ECPs will be carried over to the next CCB.
- Assign action items and monitor progress to completion.
- Develop and publish CCB meeting minutes to reflect the CCB discussions and decisions.
- Seek voting members' consensus and decisions on urgent out-of-cycle ERs/ECPs that must be addressed before the next regularly scheduled CCB meeting.
- Share all approved ERs and ECPs with the National Leadership Command Capability (NLCC) Executive Management Board (EMB).

5.2 CCB Voting Members

- Represent the interests of their organization's DCL systems role by attending CCB meetings, voting and responding to advance status request and recommendations from the CCB Chair.
- Maintain personal contact information and provide availability for attendance at scheduled meetings using the CCB SharePoint site. If unable to personally attend a scheduled meeting, arrange for a qualified and empowered government representative to attend.
- Complete all assigned CCB tasks in a timely manner.

5.3 Configuration Management Subcommittee

- Maintain the DCL Systems CM Plan.
- Develop and publish the process for submitting DCL system ERs and ECPs in the DCL systems portal.
- Establish and maintain the DCL systems ER and ECP database that contains the history of each DCL systems ER and ECP submitted for CCB consideration. This will include a prioritization list of ERs and ECPS resulting from the previous DCL systems CCB activities that includes whether the ER or ECP was approved, rejected or deferred and if approved, the anticipated DCL systems scheduled implementation date.
- Prepare ERs and ECPs for consideration by the CCB. Seek, receive, record, evaluate, categorize and prioritize DCL Systems ERs and ECPs from stakeholders and users. The results of these activities are:
  - The aggregation of similar/duplicate ERs and ECPs into single ERs and ECPs respectively and maintain an audit trail of the aggregation.
  - Provide aggregated ERs and ECPs to all voting CCB Members no later than six weeks prior to the next scheduled CCB meeting.
  - The evaluation of the proposed ERs and ECPs as to the priority of the requested change(s), the impact on business processes and policies, and the relationship to already approved ECPs.

- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Ensure all CCB approved ERs and ECPs are approved by the AO before implementation.
- Implement, with support from the CCB Member Technical and Engineering, the ERs and ECPs in accordance with the CCB approved plan and schedule.

5.4 Technical and Engineering Subcommittee

- Build and maintain the DCL Risk Management Framework (RMF) package and gain approval from the Authorizing Official.
- Evaluate ERs and ECPs provided by the Configuration Management Subcommittee for technical feasibility and impact to the technical capabilities of the DCL systems CIs.
- Provide an estimate of the resources (in consistent units of measure) required to implement ERs and ECPs across the DCL systems CIs.
- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Provide support for the implement the ERs and ECPs in accordance with the CCB approved plan and schedule.

5.5 Operations and Maintenance Subcommittee

- Provide documentation and artifacts to the Technical and Engineering Subcommittee for the Risk Management Framework package.
- Evaluate ERs and ECPs provided by the CCB Member, Planning, Programming and Budget for supportability by assigned operation and maintenance units and impact to the supportability of all DCL systems CIs.
- An estimate of the additional resources (in consistent units of measure) required to operate and maintain all DCL systems CIs due to the ERs and ECPs.
- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Provide support for the implementation of ERs and ECPs in accordance with the CCB approved plan and schedule

6.0 Decision Making Process, Communicating, Revisions & Authorizations

6.1 Decision Making Process

- Each CCB voting member will present their evaluation of the proposed ERs and ECPs.
- CCB non-voting members may present additional information for each of the ERs and ECPs to the CCB.

- The CCB chair will call for a vote on each ER and ECP.
- An affirmative vote by the majority of voting members participating in the CCB meeting will be required to approve DCL systems ERs or ECPs.
- If an ER or ECP requires an urgent out-of-cycle decision that must be addressed before the next regularly scheduled CCB meeting, the CCB Chair may contact the individual CCB voting members to solicit their vote individually immediately. Any ER or ECP approved by such a vote must be re-approved at the next official CCB meeting.
- All CCB voting members present at the CCB will sign the annotated list of ERs and ECPs affirming the votes for each ERs or ECPs as approved, rejected or deferred.
- The CCB will assign as an action item responsibility for implementation of each approved ER or ECP to the Configuration Management Subcommittee.
- Other CCB voting members may be assigned action items to support the Configuration Management Subcommittee with implementation of any approved ERs or ECPs.

6.2 Communications

- The Configuration Management Subcommittee will post all ER or ECP CCB decisions to the DCL systems portal site.
- The Configuration Management Subcommittee will inform the individual submitting agency’s point of contact for each ER or ECP submission of the CCB’s decision on the ER or ECP in writing.
- Each CCB voting member will provide advance status on ongoing ERs, ECPs, Schedule Releases, and action items to the CCB Chair bi-weekly.

6.3 Revisions

This is the original version of the DCL systems CCB Charter.

6.4 Authorization

The Director, Networks, Services & Strategy, Directorate, CIO/G-6 approve this charter effective dd mmm yy.

This page intentionally blank.

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC

3 APR 20

MEMORANDUM THRU

Commanding General (NETC-SFC-CG), 7th Signal Command (Theater), 423 22nd Street, Building 21715, Fort Gordon, GA 30905-5832

Commanding General (NETC-CG), Network Enterprise Technology (NETCOM), 2133 Cushing Street, Fort Huachuca, AZ 85613

Commanding General (ARCC-CG), United States Army Cyber Command (ARCYBER), 8825 Beulah Street, Fort Belvoir, VA 22060

FOR Director, Networks, Services and Strategy Directorate, CIO/G-6, (SAIS) Pentagon, DC 20310

SUBJECT: Direct Communications Link (DCL) Configuration Control Board (CCB)

1. The purpose of this memorandum is to request the restart of the Configuration Control Board (CCB) and its chartered governance process related to the Direct Communications Link (DCL) and its subcomponents. The Detrick Earth Station (DES), the government-to-government (US to Russia) satellite ground station subcomponent of the DCL, is operated and maintained by this command.

2. Previously, the Direct Communications Link and its subsystems were governed by a configuration control board chaired by the AONS Directorate with the 21st Signal Brigade as the CCB's secretariat. This governing body provided the necessary interactions among stakeholders and helped shape the systems we have today. With the ongoing and emerging changes in the DCL configurations, I believe it is appropriate that this CCB be restarted; or as a minimum be integrated into another existing governing structure.

3. Having a standing forum to review and collaborate on emerging changes will have benefits to the community at large and make the success of the systems more assured. I look forward to working with you on this effort.

4. Team 21 - "Edge of the Sword."

[redacted] Digitally signed by [redacted]
Date: 2020.04.03 [illegible]

[redacted]
COL, SC
Commanding

DEPARTMENT OF THE ARMY
US ARMY SIGNAL ACTIVITY – FORT DETRICK
1678 NELSON STREET
FORT DETRICK, MD 21702-5002

REPLY TO
ATTENTION OF

NETC-SYD-A

02 April 2020

MEMORANDUM FOR RECORD

SUBJECT: Fire Detection and Suppression Site Survey Inspection

1. The Detrick Earth Station (DES); 1650 Porter Street, Fort Detrick, MD 21702, will undergo a Fire Detection and Suppression Site Survey Inspection by the Fort Detrick Fire Department and Baltimore Fire Protection Equipment (BFPE) on 06 April 2020.

2. The inspection will be conducted by the Fort Detrick Fire Department Assistant Fire Chief – Prevention, [redacted], and Mr. [redacted] of BFPE. The survey will determine if the fire detection system mitigates the requirement for a fire suppression system.

3. POC is the undersigned; [redacted]mail.mil; (301) 619-3604

[redacted]

Digitally signed by
[redacted]
Date: 2020.04.02 16:50:18 -04'00'

CXO, USASA-DET

SUMMARY SHEET	COORD LEVEL GO/FO	TRACKING NUMBER

TO	ACTION	TYPED NAME	CONCUR	INITIALS	DATE	TO	ACTION	TYPED NAME	CONCUR	INITIALS	DATE
1. IES	Review	Mr. [redacted]	Yes	[redacted]		11.					
2. IE	Coord	CAPT [redacted]	Yes	[redacted]		12.					
3. IE	Coord	[redacted]	Yes	[redacted]		13.					
4. IE	Review	Mr. [redacted]	Yes	[redacted]		14.					
5. OC	Coord	Ms. [redacted]				15.					
6. OC	Review	Mr. [redacted]	Yes	[redacted]		16.					
7. RE	Coord	Ms. [redacted]				17.					
8. RE	Coord	Ms. [redacted]				18.					
9. RE	Approve	Mr. [redacted]				19.					
10.						20.					

SUBJECT DCL AO approval for NSA network assessment.	SUSPENSE DATE: 2020-03-04

SUMMARY

PURPOSE: 1) Assign an Authorizing Official (AO) to approve Washington-Moscow DCL NSA vulnerability/ security assessment. 2) NSA requires DCL AO to sign Annex_SVA_DISA and Terms_and_Conditions Documents before the start of the assessment of different network elements on 23 March 2020.

BACKGROUND:
a) Washington-Moscow Direct Communications Link (DCL) network is managed by DISA IE8.
b) DISA assigned as the US Competent Agency responsible to implement 2008 Secure Communications System (SCS) agreement.
c) Serve as Principal Office of Responsibility (POR) and the Program Management Office (PMO) for engineering, management, and validation of user requirements connected to or traversing DCL network
d) Designated to establish, operate, & maintain DCL COMSEC account (ASD(NII)/DoD CIO 28 Apr 2009).
e) Exercise program management and technical oversight of all activities pertaining to the SNLC and DCL UTCP systems.
f) Most of US Site Operators/Maintainers are DISA personnel.
g) DCL currently presumes Close Restricted Network and exemption requirement of DoDD 8500.1 paragraph 2.3.
h) No part of the current DCL network has been accredited
i) No DoDIN Connectivity (to include current DCL Satellites)
j) No visibility on the Russia components of the network

ACTION OFFICER [redacted]	OFFICE CODE IE8	PHONE NUMBER 301-225-4800
SIGNATURE [redacted] Digitally signed by [redacted] Date: 2020.02.27 08:45:19 -05'00'	DATE PREPARED 2/25/20	

SUMMARY (Continued)

Recommend:
Assign Mr. [redacted] (RE) as the AO for DCL network. Mr. [redacted] signs required NSA assessment documents.

Enclosures:
a) Annex_SVA_DISA
b) Terms_and_Conditions
c) DISA General Counsel Approval Email (NSA Assesment)
d) DCL_Top_Level_Block_Diagram_APB_1_31_2020

COMMENTS *(required by all who select "no" under concur)*

TAB S

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC   3 APR 20

MEMORANDUM THRU

Commanding General (NETC-SFC-CG), 7th Signal Command (Theater), 423 22nd
    Street, Building 21715, Fort Gordon, GA 30905-5832

Commanding General (NETC-CG), Network Enterprise Technology (NETCOM), 2133
    Cushing Street, Fort Huachuca, AZ 85613

Commanding General (ARCC-CG), United States Army Cyber Command (ARCYBER),
    8825 Beulah Street, Fort Belvoir, VA 22060

FOR Director, Networks, Services and Strategy Directorate, CIO/G-6, (SAIS) Pentagon,
DC 20310

SUBJECT: Direct Communications Link (DCL) Configuration Control Board (CCB)

1. The purpose of this memorandum is to request the restart of the Configuration Control Board (CCB) and its chartered governance process related to the Direct Communications Link (DCL) and its subcomponents. The Detrick Earth Station (DES), the government-to-government (US to Russia) satellite ground station subcomponent of the DCL, is operated and maintained by this command.

2. Previously, the Direct Communications Link and its subsystems were governed by a configuration control board chaired by the AONS Directorate with the 21st Signal Brigade as the CCB's secretariat. This governing body provided the necessary interactions among stakeholders and helped shape the systems we have today. With the ongoing and emerging changes in the DCL configurations, I believe it is appropriate that this CCB be restarted; or as a minimum be integrated into another existing governing structure.

3. Having a standing forum to review and collaborate on emerging changes will have benefits to the community at large and make the success of the systems more assured. I look forward to working with you on this effort.

4. Team 21 - "Edge of the Sword."

[redacted] Digitally signed by [redacted]
Date: 2020.04.03 [illegible]

[redacted]
COL, SC
Commanding

TAB T

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC

14 May 20

MEMORANDUM FOR RECORD

SUBJECT: Update 1 - Implementation of Findings for Direct Communications Link (DCL) Detrick Earth Station (DES)

1. Reference Memorandum, 21st Signal Brigade, NETC-SYC, 3 Apr 20, subject: Implementation of Findings for Direct Communications Link (DCL) Detrick Earth Station (DES) (enclosed).

2. This memorandum provides an update to the activities with respect to the items of the reference.

3. Activities:

a. The report from the Fort Detrick Fire Marshal's inspection on 6 April (reference par. 3d) is enclosed.

b. On 6 May, I briefed MG David T. Isaacson, Director, Network, Services & Strategy, CIO/G-6, about the reestablishment of the CCB. I covered the CCB re-start memorandum routing to him, the draft Charter, the history of the CCB, and the way forward.

c. On 12 May we created the collaboration environment for the CCB and initiated the first meeting with all of the stakeholders and members. This meeting will be on 21 May. The agenda is enclosed.

4. Team 21 - "Edge of the Sword."

[redacted] Digitally signed by:
[redacted]
Date: 2020.05.14 07:41:35 -04'00'

[redacted]
COL, SC
Commanding

3 Encls
1. Implementation Memo, 3 Apr 20
2. Fire Marshal Memo, 6 Apr 20
3. Agenda, CCB Meeting 21 May 20

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC

3 Apr 20

[redacted] Digitally signed by [redacted]
Date: [illegible]

MEMORANDUM THRU Commanding General (NETC-SFC-CG), 7th Signal Command (Theater), 423 22nd Street, Building 21715, Fort Gordon, GA 30905-5832

FOR Commanding General (NETC-CG), Network Enterprise Technology (NETCOM), 2133 Cushing Street, Fort Huachuca, AZ 85613

SUBJECT: Implementation of Findings for Direct Communications Link (DCL) Detrick Earth Station (DES)

1. Reference Memorandum, Network Enterprise Technology Command (NETCOM), NETC-CS, 26 Mar 20, subject: Approval of Report of Investigation for Whistleblower Investigation Concerning Office of Special Counsel Referral DI-17-2168, Department of the Army, 1st Personnel Command, Washington-Moscow Direct Communications Link, Detrick Earth Station, Fort Detrick, Maryland.

2. This memorandum provides a response and timeline for the items listed in par. 2 of the reference.

3. Detailed responses:

a. "*Complete the Configuration Control Board (CCB) charter that was initiated by a previous 21st Signal Brigade Commander.*" Completed, see enclosure 1. The charter draft is prepared for review upon the initiation of the CCB of item 3b below.

b. "*Staff a memorandum through 7th Command, NETCOM, and ARCYBER, to CIO/G-6 requesting that the CIO/G-6 chair the CCB in accordance with Army regulation.*" Completed, see enclosure 2. The memorandum, NETC-SYD, 3 Apr 20, subject: Direct Communications Link (DCL) Configuration Control Board (CCB) is routing.

c. "*Request Fort Detrick Fire Marshal conduct an inspection of the building.*" Completed, see enclosure 3. The request of the Fort Detrick Fire Marshal was made on 2 APR 20. The inspection is scheduled for 6 Apr 20.

d. "*Initiate the risk management process requirements at Detrick Earth Station in accordance with the new risk management framework.*" Completed, see enclosure 4. Mr. [redacted], Chief, Senior National Leadership Communications Division (OPC/IE/IE8), DISA, provided the document at enclosure 4 (DISA Form 9, 25 Feb 20, subject: DCL AO Approval for NSA Network Assessment). It is his determination that Mr. [redacted]., SES, RME/RE/CIO, Risk Management Executive/

Authorizing Official, of DISA is the Authorizing Official (AO). Mr. [redacted] submission shows the initiation of the accreditation of the DCL/DES within the DISA AO's purview.

4. Team 21 - "Edge of the Sword."

[redacted] Digitally signed by [redacted]
Date: 2020.04.03 15:39:08 -04'00'

[redacted]
COL, SC
Commanding

4 Encls
1. Draft CCB Charter
2. CCB Restart Memo, 3 Apr 20
3. Fire Marshall Memo, 2 Apr 20
4. DISA Form 9, 25 Feb 20

Department of the Army
CIO/G-6

Direct Communications Link Configuration Control Board Charter

"Peace Through Reliable Communications"

May 2020

Table of Contents

Charter, Direct Communications Link Configuration Control Board

1.0 Authorities, Objectives and Scope

The Direct Communications Link (DCL) Configuration Control Board (CCB) is chartered through the Army Chief Information Officer (CIO)/G-6 to successfully identify engineering plans, configuration standards and designs, and implementations that support operational requirements for the DCL. The CCB will work to ensure interoperability and synchronization between all stakeholders.

This charter establishes the Army DCL CCB and assigns responsibilities for establishing and maintaining of technical and functional baselines for the system. The Army DCL CCB will operate in an integrated and disciplined manner to provide a structured and streamlined control process for managing the assigned products and services throughout their intended life cycle. Life cycle configuration management through the CCB ensures that all changes are visible, that any potential safety, security and operational impacts are properly addressed, and that technical and programmatic direction across the DCL system's products, services and interfaces are consistent.

1.1 Authorities

1.1.1 USD C4I

Under Secretary of Defense for Command, Control, Communications and Intelligence Memorandum Subject: Upgrade to the US/USSR Direct Communications Link (DCL) dated 14 March 1984 designated the Army as Lead Military Department for the DCL.

1.1.2 NSD-301

National Security Directive – 301 (NSD-301), dated February 1988, assigned life cycle support responsibility, on a reimbursable basis, to the Department of the Army for the Nuclear Risk Reduction Center (NRRC) program.

1.1.3 ASD C41

Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandum Subject: Designation of Army as Lead Military Department (LMD) for the Direct Communications Link (DCL), the Continuous Communications Link (CCL) and the Government to Government Communications Links (GGCLs) dated 28 July 2000 reaffirmed the Army's designation as LMD for the DCL, CCL and GGCLs.

1.1.4 ASD NII

Assistant Secretary of Defense for Networks and Information Integrations / DoD Chief Information Officer (ASD(NII)/DoD CIO) Memorandum Subject: Communications With Other Nations (CWON) dated 28 April 2009 established the National Leadership

Command Capability (NLCC) Executive Management Board (EMB) to coordinate CWON issues.

1.1.5 DODD 8000.01

Department of Defense Directive 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), dated 27 July 2017.

1.1.6 AR 25-1

Army Regulation 25-1 Information Management, Army Information Technology, dated 15 July 2019.

1.2 Objectives

- Serve as the focal point for Direct Communications Link activities
- Review, coordinate, synchronize and approve system changes
- Ensure Direct Communications Link cyber compliance
- Promote the efficient operation of cross-functional and cross-organizational business processes

1.3 Scope

The DLC CCB operates under the authority and in support of the Army Chief Information Officer/G-6 (CIO/G-6) and the Defense Information Systems Agency (DISA) for support of Communications With Other Nations (CWON) Systems. The approving authority for the CCB Charter is the Army CIO/G-6. The CCB determines DCL future capability development and prioritizes, approves, plans and integrates requests for change into the current and future systems throughout the life cycle and ensures all efforts are coordinated with the National Leadership Command Capability (NLCC) Executive Management Board (EMB). The CCB represents the interests of all stakeholders of the DCL systems and/or may be affected by changes to the DCL configuration item (CI) baselines.

The scope of the CCB activities include:

- IT engineering in support of the DCL
- Review and evaluation of proposed DCL lifecycle upgrades and design solutions
- Activities and engineering related to Cyber, NetOps, networks, operations management and defense of the DCL systems and services
- Development, oversight and maintenance of policies, standards and procedures for the use of the DCL
- Determination of whether projects and plans align and comply with the published IT standards and policies
- Determination to include or exclude new technologies and services into the DCL infrastructure

- Support the development and management of DCL technical architecture blueprints and standards
- Architecture technical compliance reviews
- Recommendations to the Enterprise Authorizing Official

2.0 Membership

The DCL CCB is comprised of voting members and non-voting members. Voting members represent the community's interests in the following areas; Policy; Planning, Programming and Budget; Technical and Engineering; Operations and Maintenance. Non-voting members of the CCB represent the other Federal Agencies and User Communities that provide information and assistance to the CCB. The Director, Networks, Systems & Services Directorate, Army CIO/G-6 has been designated as the CCB Chair. The DISA Communications With Other Nations (CWON) Program Manager is designated as the CCB Deputy Chair. Voting members must be empowered by their organizations, by memorandum, with the authority to make decisions on all matters coming before the CCB.

All voting members of the CCB are expected to be present for all CCB meetings. Geographically dispersed members may participated by video teleconference or telephone. Voting members, with the prior approval of the CCB Chair, may designate, by memorandum, an alternate representative in those instances when the primary representative is not available. A quorum necessary for conducting CCB functions is reached when 80% of the voting members are represented at the meeting.

2.1 Chair

Director, Networks, Services & Strategy, Directorate, CIO/G-6.

2.2 Deputy

Program Manager, Communications With Other Nations (CWON), DISA.

2.3 Secretary

Civilian Deputy to the Commander, 21st Signal Brigade, Fort Detrick, Maryland.

2.4 Membership

2.4.1 Voting Members

Representatives for the following agencies/organizations constitute the voting members of the DCL CCB.

- Army CIO/G-6, Director, Networks, Services & Strategy, Directorate, CIO/G-6, CCB Chair

- Program Manager, Communications With Other Nations (CWON), DISA, Deputy Chair
- Civilian Deputy to the Commander, 21st Signal Brigade, Secretary
- Army Project Manager Defense Communications and Army Transmission System (PM DCATS), CCB Member, Programming and Budget
- Army Information Systems Engineering Command (ISEC), CCB Member, Technical and Engineering
- Army Network Enterprise Technology Command (NETCOM) Assistant Chief of Staff (ACofS) G-3/5/7, CCB Member, Operations and Maintenance

2.4.2 Non-voting Members

All non-voting members may participate in the CCB at their discretion. Information presented by the non-voting members will be considered by the CCB prior to final decisions.

Representatives from the following agencies/organizations constitute the non-voting members of the DCL CCB.

- Chief, Washington-Moscow Direct Communications Link (MOLINK), J3, Joint Staff
- Staff Director, Department of State Bureau of Arms Control, Verification, and Compliance (AVC) Nuclear Risk Reduction Center (NRRC)
- NRRC Branch, Department of State Information Resource Management (IRM)
- Telecommunications Division, DISA White House Communications Agency (WHCA)
- Information Assurance Manager, CWON, DISA

3.0 Duties of the Board Members

3.1 The Chair

- Direct all CCB activities
- Call and chair (i.e., lead) CCB meetings
- Assign actions and tasks
- Establish subordinate tiger teams and integrated process teams (IPTs) as needed
- Approve agendas and minutes
- Ensure dissemination and coordination of information to all appropriate stakeholders
- Identify, prioritize and approve initiatives and decisions for submission to the CCB
- Resolve other issues as required

3.2 The Deputy

- Support the Chair and act as the Chair in his absence

- Coordinate and synchronize member activities in support of the objectives and scope of the CCB
- Be the initial focal point for resolution of engineering related issues that arise
- Provide advice and counsel to the Chair on Board matters
- Disseminate specific requirements for data and other actions on behalf of the Board
- Structure issues and ensure proper representation on items before the Board
- Monitor and track follow-on actions taken to ensure that decisions reached and assignments made by the Board Chair/Board are implemented properly
- Support and coordinate the activities of the Board's subordinate bodies

3.3 The Secretary

- Publish agendas, coordinate and schedule meetings at the Chair's direction
- Facilitate the Chair and Deputy to coordinate activities during actual meetings
- Develop and publish the official minutes, resolutions and actions of the CCB
- Ensure all security rules and regulations regarding classified meetings and documents are followed
- Assemble, prepare and distribute material on matters under consideration by the Board at least three working days in advance
- Maintain collaboration sites, minutes, agendas, wikis, blogs and knowledge centers
- Compile and maintain contact lists for the Board members, their coordinating staffs and any subordinate bodies

3.4 CCB Members

- Represent organizational positions on CCB issues
- Sponsor items and issues for meetings, including preparation of position papers, read-ahead materials and presentation of briefings
- Identify and nominate agenda items and issues to the Chair for consideration
- Ensure dissemination and coordination of CCB information to all appropriate organizational stakeholders and staffs working source material (e.g., technical documents) as necessary to ensure open collaboration
- Convey and support CCB positions and decisions to their organizations
- Execute actions and tasks as directed by the Chair
- Ensure member organizations are represented on appropriate CCB subordinate bodies, e.g., Tiger Teams
- Designate an alternate CCB representative responsible for attending meetings in the absence of the principal representative
- Designate members and subject matter experts for standing and ad-hoc working groups
- Review minutes

4.0 Subordinate Bodies

Tiger Teams and IPTs are organized and participate as needed within the CCB.

The Purpose of the Tiger Team/IPT is to act as an SME group to facilitate senior level decision-making to this end:

1. Provide advice to the CCB to help make presentations more concise, accurate and understandable.

2. Identify potential conflicts and work to obtain resolution at the lowest level.

3. Champion CCB issues and positions within military organizations to gain working level support.

4. Disseminate CCB information to all appropriate organizational stakeholders and staffs working documents as necessary to ensure open collaboration.

Tiger Teams/IPTs report to the CCB. IPTs will be formed for efforts that are considered “longer term” in nature, e.g., for efforts that are expected to last 6 months or longer. The CCB will direct the creation of IPTs. The CCB will designate the leads and membership of the IPT, following the guidance given by the CCB.

Tiger Teams will be formed for efforts that are considered “shorter term” in nature, e.g., for efforts that are expected to last less than 6 months. Tiger Teams will normally support and report to IPT leads.

5.0 Operating Procedures

5.1 Leadership

The DCL CCB will meet quarterly or at the call of the CCB Chair. The DCL CCB will establish a configuration management (CM) plan that documents all CM roles, responsibilities and procedures for implementation of CCB approved Engineering Requests (ERs) and Engineering Change Proposals (ECPs).

The CCB Chair, with support from the CCB secretary, will:

- Establish and maintain the DCL CCB portal site that will be used to disseminate and collect CCB information and data.
- Schedule CCB meetings and locations.
- Publish meeting agendas.
- Provide advance status on ERs, ECPs, Schedule Releases, and Independent Verification and Validation (IV&V) activities and other items to be addressed by the CCB no later than three weeks prior to a scheduled CCB meeting.

- Request CCB voting members review the advance information and formulate a vote on CCB Chair recommendations that are not anticipated to be controversial.
- Conduct CCB meetings and record meeting minutes to include an annotated list of ERs and ECPs as approved, rejected, or deferred.
- Approved ERs and ECPs will be scheduled for implementation as part of the overall DCL schedule. Deferred ERs and ECPs will be carried over to the next CCB.
- Assign action items and monitor progress to completion.
- Develop and publish CCB meeting minutes to reflect the CCB discussions and decisions.
- Seek voting members' consensus and decisions on urgent out-of-cycle ERs/ECPs that must be addressed before the next regularly scheduled CCB meeting.
- Share all approved ERs and ECPs with the National Leadership Command Capability (NLCC) Executive Management Board (EMB).

5.2 CCB Voting Members

- Represent the interests of their organization's DCL systems role by attending CCB meetings, voting and responding to advance status request and recommendations from the CCB Chair.
- Maintain personal contact information and provide availability for attendance at scheduled meetings using the CCB SharePoint site. If unable to personally attend a scheduled meeting, arrange for a qualified and empowered government representative to attend.
- Complete all assigned CCB tasks in a timely manner.

5.3 Configuration Management Subcommittee

- Maintain the DCL Systems CM Plan.
- Develop and publish the process for submitting DCL system ERs and ECPs in the DCL systems portal.
- Establish and maintain the DCL systems ER and ECP database that contains the history of each DCL systems ER and ECP submitted for CCB consideration. This will include a prioritization list of ERs and ECPS resulting from the previous DCL systems CCB activities that includes whether the ER or ECP was approved, rejected or deferred and if approved, the anticipated DCL systems scheduled implementation date.
- Prepare ERs and ECPs for consideration by the CCB. Seek, receive, record, evaluate, categorize and prioritize DCL Systems ERs and ECPs from stakeholders and users. The results of these activities are:
  - The aggregation of similar/duplicate ERs and ECPs into single ERs and ECPs respectively and maintain an audit trail of the aggregation.
  - Provide aggregated ERs and ECPs to all voting CCB Members no later than six weeks prior to the next scheduled CCB meeting.
  - The evaluation of the proposed ERs and ECPs as to the priority of the requested change(s), the impact on business processes and policies, and the relationship to already approved ECPs.

- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Ensure all CCB approved ERs and ECPs are approved by the AO before implementation.
- Implement, with support from the CCB Member Technical and Engineering, the ERs and ECPs in accordance with the CCB approved plan and schedule.

5.4 Technical and Engineering Subcommittee

- Build and maintain the DCL Risk Management Framework (RMF) package and gain approval from the Authorizing Official.
- Evaluate ERs and ECPs provided by the Configuration Management Subcommittee for technical feasibility and impact to the technical capabilities of the DCL systems CIs.
- Provide an estimate of the resources (in consistent units of measure) required to implement ERs and ECPs across the DCL systems CIs.
- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Provide support for the implement the ERs and ECPs in accordance with the CCB approved plan and schedule.

5.5 Operations and Maintenance Subcommittee

- Provide documentation and artifacts to the Technical and Engineering Subcommittee for the Risk Management Framework package.
- Evaluate ERs and ECPs provided by the CCB Member, Planning, Programming and Budget for supportability by assigned operation and maintenance units and impact to the supportability of all DCL systems CIs.
- An estimate of the additional resources (in consistent units of measure) required to operate and maintain all DCL systems CIs due to the ERs and ECPs.
- Prepare draft recommendations for ERs and ECPs to be addressed at the next CCB meeting to the CCB Chair for release to the CCB voting members no later than four weeks prior to the next scheduled CCB meeting.
- Provide support for the implementation of ERs and ECPs in accordance with the CCB approved plan and schedule

6.0 Decision Making Process, Communicating, Revisions & Authorizations

6.1 Decision Making Process

- Each CCB voting member will present their evaluation of the proposed ERs and ECPs.
- CCB non-voting members may present additional information for each of the ERs and ECPs to the CCB.

- The CCB chair will call for a vote on each ER and ECP.
- An affirmative vote by the majority of voting members participating in the CCB meeting will be required to approve DCL systems ERs or ECPs.
- If an ER or ECP requires an urgent out-of-cycle decision that must be addressed before the next regularly scheduled CCB meeting, the CCB Chair may contact the individual CCB voting members to solicit their vote individually immediately. Any ER or ECP approved by such a vote must be re-approved at the next official CCB meeting.
- All CCB voting members present at the CCB will sign the annotated list of ERs and ECPs affirming the votes for each ERs or ECPs as approved, rejected or deferred.
- The CCB will assign as an action item responsibility for implementation of each approved ER or ECP to the Configuration Management Subcommittee.
- Other CCB voting members may be assigned action items to support the Configuration Management Subcommittee with implementation of any approved ERs or ECPs.

6.2 Communications

- The Configuration Management Subcommittee will post all ER or ECP CCB decisions to the DCL systems portal site.
- The Configuration Management Subcommittee will inform the individual submitting agency’s point of contact for each ER or ECP submission of the CCB’s decision on the ER or ECP in writing.
- Each CCB voting member will provide advance status on ongoing ERs, ECPs, Schedule Releases, and action items to the CCB Chair bi-weekly.

6.3 Revisions

This is the original version of the DCL systems CCB Charter.

6.4 Authorization

The Director, Networks, Services & Strategy, Directorate, CIO/G-6 approve this charter effective dd mmm yy.

This page intentionally blank.

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

NETC-SYC

3 APR 20

MEMORANDUM THRU

Commanding General (NETC-SFC-CG), 7th Signal Command (Theater), 423 22nd Street, Building 21715, Fort Gordon, GA 30905-5832

Commanding General (NETC-CG), Network Enterprise Technology (NETCOM), 2133 Cushing Street, Fort Huachuca, AZ 85613

Commanding General (ARCC-CG), United States Army Cyber Command (ARCYBER), 8825 Beulah Street, Fort Belvoir, VA 22060

FOR Director, Networks, Services and Strategy Directorate, CIO/G-6, (SAIS) Pentagon, DC 20310

SUBJECT: Direct Communications Link (DCL) Configuration Control Board (CCB)

1. The purpose of this memorandum is to request the restart of the Configuration Control Board (CCB) and its chartered governance process related to the Direct Communications Link (DCL) and its subcomponents. The Detrick Earth Station (DES), the government-to-government (US to Russia) satellite ground station subcomponent of the DCL, is operated and maintained by this command.

2. Previously, the Direct Communications Link and its subsystems were governed by a configuration control board chaired by the AONS Directorate with the 21st Signal Brigade as the CCB's secretariat. This governing body provided the necessary interactions among stakeholders and helped shape the systems we have today. With the ongoing and emerging changes in the DCL configurations, I believe it is appropriate that this CCB be restarted; or as a minimum be integrated into another existing governing structure.

3. Having a standing forum to review and collaborate on emerging changes will have benefits to the community at large and make the success of the systems more assured. I look forward to working with you on this effort.

4. Team 21 - "Edge of the Sword."

[redacted]

[redacted]
COL, SC
Commanding

Fort Detrick Fire and Emergency Services
1419 Sultan Drive
Fort Detrick, MD 21702-5000
Phone 301-619-2528
Fax 301-619-2163

Date: 4/13/2020
Mr. [redacted]
CXO, 298th Signal Co.
USAG/Ft. Detrick

Mr. [redacted],

I am writing this in response to your questions regarding Building 1650 and whether it is in compliance with all the applicable codes and standards related to fire and life safety.

As you are aware back in 2015 it was identified that the facility in question did in fact lack the appropriate level of fire detection, however we were able to get this deficiency corrected utilizing the DPW/Installation Fire Protection Maintenance Contract and installed a state of the art, fully addressable fire alarm system and later we were able to provide detection in the foreign equipment sheds to provide supervision of those assets as well.

In regards to your question on fire suppression and that facilities lack thereof, while it would be recommended to install a wet sprinkler system and supplemental clean agent system in this facility, it is not required by the applicable regulations or codes based on the date of the facilities construction, and it would only become a requirement if at any time the facility was renovated and those costs of the renovation exceeded 50% of the original construction cost.

In regards to fire & life safety compliance of the remainder of the facility. This building is in compliance with all DoD & Army regulations as well as any and all applicable NFPA codes and standards for an existing business occupancy such as this.

If you have any further questions or if I can be assistance in any other way please do not hesitate to contact me.

[redacted]

[redacted]
Assistant Fire Chief - Prevention
Ft. Detrick/Forest Glen Fire & Emergency Services

Fort Detrick Fire and Emergency Services
1419 Sultan Drive
Fort Detrick, MD 21702-5000
Phone 301-619-2528
Fax 301-619-2163

SUMMARY SHEET	COORD LEVEL	GO/FO	TRACKING NUMBER

TO	ACTION	TYPED NAME	CONCUR	INITIALS	DATE	TO	ACTION	TYPED NAME	CONCUR	INITIALS	DATE
1. IES	Review	Mr. [redacted] [redacted]	Yes	[redacted]		11.					
2. IE	Coord	CAPT [redacted] [redacted]	Yes	[redacted]		12.					
3. IE	Coord	Mr [redacted]	Yes	[redacted]		13.					
4. IE	Review	Mr. [redacted]	Yes	[redacted]		14.					
5. OC	Coord	Ms. [redacted]				15.					
6. OC	Review	Mr. [redacted]	Yes	[redacted]		16.					
7. RE	Coord	Ms. [redacted]				17.					
8. RE	Coord	Ms. [redacted]				18.					
9. RE	Approve	Mr. [redacted] [redacted]				19.					
10.						20.					

SUBJECT

DCL AO approval for NSA network assessment.

SUSPENSE DATE:

2020-03-04

SUMMARY

PURPOSE: 1) Assign an Authorizing Official (AO) to approve Washington-Moscow DCL NSA vulnerability/ security assessment. 2) NSA requires DCL AO to sign Annex_SVA_DISA and Terms_and_Conditions Documents before the start of the assessment of different network elements on 23 March 2020.

BACKGROUND:

a) Washington-Moscow Direct Communications Link (DCL) network is managed by DISA IE8.

b) DISA assigned as the US Competent Agency responsible to implement 2008 Secure Communications System (SCS) agreement.

c) Serve as Principal Office of Responsibility (POR) and the Program Management Office (PMO) for engineering, management, and validation of user requirements connected to or traversing DCL network

d) Designated to establish, operate, & maintain DCL COMSEC account (ASD(NII)/DoD CIO 28 Apr 2009).

e) Exercise program management and technical oversight of all activities pertaining to the SNLC and DCL UTCP systems.

f) Most of US Site Operators/Maintainers are DISA personnel.

g) DCL currently presumes Close Restricted Network and exemption requirement of DoDD 8500.1 paragraph 2.3.

h) No part of the current DCL network has been accredited

i) No DoDIN Connectivity (to include current DCL Satellites)

j) No visibility on the Russia components of the network

ACTION OFFICER [redacted]	OFFICE CODE IE8	PHONE NUMBER 301-225-4800
SIGNATURE [redacted] Digitally signed by [redacted] Date: 2020.02.27 08:45:19 -05'00'	DATE PREPARED 2/25/20	

SUMMARY (Continued)

Recommend:
Assign Mr. [redacted] (RE) as the AO for DCL network. Mr [redacted] signs required NSA assessment documents.

Enclosures:
a) Annex_SVA_DISA
b) Terms_and_Conditions
c) DISA General Counsel Approval Email (NSA Assesment)
d) DCL_Top_Level_Block_Diagram_APB_1_31_2020

COMMENTS *(required by all who select "no" under concur)*

DEPARTMENT OF THE ARMY
US ARMY SIGNAL ACTIVITY – FORT DETRICK
1678 NELSON STREET
FORT DETRICK, MD 21702-5002

REPLY TO
ATTENTION OF:

NETC-SYD-A 02 April 2020

MEMORANDUM FOR RECORD

SUBJECT: Fire Detection and Suppression Site Survey Inspection

1. The Detrick Earth Station (DES); 1650 Porter Street, Fort Detrick, MD 21702, will undergo a Fire Detection and Suppression Site Survey Inspection by the Fort Detrick Fire Department and Baltimore Fire Protection Equipment (BFPE) on 06 April 2020.

2. The inspection will be conducted by the Fort Detrick Fire Department Assistant Fire Chief – Prevention, Michael Custer, and Mr. [redacted] of BFPE. The survey will determine if the fire detection system mitigates the requirement for a fire suppression system.

3. POC is the undersigned [redacted]; (301) 619-3604

[redacted] Digitally signed by
[redacted]
Date: 2020.04.02 18:50:12 -04'00'

CXO, USASA-DET

DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1435 PORTER STREET
FORT DETRICK MD 21702-5046

Agenda

Direct Communications Link Configuration Control Board Meeting
Thursday, 21 May, 1030 Eastern

Teleconference Bridge
DSN (312) [redacted], COMM (301) 909-7351, Access Code [redacted]
Documents: DCL CCB Team General Channel

Host: Network, Services & Strategy Directorate, CIO/G-6
Alternate Host: Civilian Deputy Brigade Commander, 21st Signal Brigade

1030 Roll Call

1. Introductions, Membership, & Background - Host & Milani
2. Charter Discussion - Milani
3. Battle Rhythm Discussion - Milani
4. Due Outs from September Meeting - Milani
5. Open Discussion - All
6. Recap, action item review - Milani

1200 Adjourn

21st Signal Brigade		DISA		MOLINK		ISEC		White House	
[redacted]		[redacted]		[redacted]		[redacted]		[redacted]	
[redacted]		[redacted]		[redacted]		[redacted]		[redacted]	
[redacted]		[redacted]		NSS, CIO/G-6		[redacted]		State Department	
[redacted]		[redacted]				[redacted]		[redacted]	
[redacted]		[redacted]				[redacted]		[redacted]	
[redacted]		[redacted]				[redacted]		[redacted]	
[redacted]		JSP				PM DCATS/PdM WESS		SEC	
		[redacted]				[redacted]		[redacted]	
		[redacted]				[redacted]		[redacted]	
		[redacted]						[redacted]	

"Peace Through Reliable Communications"

TAB U

SAIS-AONS [tentative publication date: 7 June 2012]

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Minutes of the Direct Communications Link (DCL) Configuration Control Board (CCB) Meeting, 22 May 2012

1. Purpose. This document conveys the discussion points, recommendations, and decisions of the DCL CCB meeting held in Pentagon room 3E609 from 1300-1500 on 22 May 2012.

2. Participants. See list at Enclosure 1.

3. Discussion points.

a. Mr. [redacted], Director of the LandWarNet Network Integration Division in Army CIO/G6, welcomed and thanked the attendants for their participation and for the ongoing mission accomplishment of their respective roles. Many offices are constantly engaged in their designated actions for management, support, and analysis of the DCL and other components of the Senior National Leader Communications (SNLC) networks. However, recent developments and the potential for a significant update in the network architecture make it necessary to bring several actions to higher levels of management for their attention and consideration.

b. Mr. [redacted] from Army CIO/G6 provided an overview of the history of DCL systems and responsibilities. He also conveyed the results of research into the primary source documents for these systems. The primary references include Presidential Decision Directives (PDDs), National Security Council (NSC) documents, DOD policies, and Army implementation guidance. Although these directives give authority and direction for each respective office to proceed with its particular responsibilities, there are key areas where the documentation is no longer up to date with regard to the US and international political environment; the leadership structure of the US customers and responsible organizations; and the range of technology in commercial and military networks. Mr. [redacted] identified three “lanes” of management and coordination, each with its particular issues and challenges: Requirements, Governance, and Implementation. The paragraphs below provide the current status, challenges, and way ahead for each management lane.

4. Requirements.

(1) Current status. Approximately 10 distinct source documents cover the national-level requirements for the DCL and associated systems. Between Dec 2011 and May 2012, Mr. [redacted] circulated a summarized list of these documents and their key provisions, using the SIPRNET because many of the files are classified.

(2) Challenges. The key challenges in this management lane include growth in end-user features that are not clearly assigned by national-level guidance. In recent years, several implementing organizations have included and/or considered enhancements that go beyond the core designated systems and capabilities expressed in the core PDD and NSC documentation. According to several source documents, any such changes should come to the Standing Subcommittee on Upgrades (SSU) for decisions, yet the SSU has not met since the 1990s. Also in the requirements lane, the classification markings on several source documents are out of date. Some elements of information are classified in US directives, apparently to preserve the range of options for US decision makers, and yet many of these elements of information have been made public through official announcements and international agreements.

(3) Discussion and way ahead. Mr. [redacted] recommended that the CCB should frame specific recommendations on updates to the governing documents, to bring them up to date with actual developments in the DCL systems. Mr. [redacted] from the 21st Signal Brigade recommended that the CCB should establish an ad-hoc working group to reexamine the source documents and develop specific recommendations on downgrading the classification levels and/or restrictions on distribution of the contents. The CCB agreed to this recommendation, and identified the CIO/G6, Information Technology Agency (ITA), 21st Signal Brigade, and DISA SNLC offices as the members of this group. The group will strive to develop a coordinated set of recommendations for presentation to a subsequent CCB meeting within 3 months.

5. Governance.

(1) Current status. Many directives address particular sub-groups of activity and sub-sections of the overall DCL network. Each respective organization has its own chain of command and its own resourcing channels for DCL-related missions. Under the CCB charter, the Engineering Working Group (EWG) is a functioning, viable group that meets at least twice each year with all US participants. The EWG also arranges for discussions with international counterparts when needed. The State Department oversees and manages the annual Technical Experts Working Group of key leaders from the US, Russia, and other partner countries. However, as noted above, the SSU is not currently an active group, and the Software Working Group (SWG) under the CCB has not held any structured events in many years. There are at least 4 different resource portfolios within the Army supporting elements of the DCL architecture.

(2) Challenges. The DCL charter was last circulated in 2008. It is out of date with regard to several participating organizations. In the absence of active engagement of the SSU, the CCB is not tied in with a higher-level group for guidance and approval. There is not a single or central office with oversight of all portfolio/investment considerations for the DCL. When more than one capability goes over a given US terrestrial circuit, it is difficult to reach consensus on improvements or termination of provisions that might be ineffective or unnecessary. Some of the guiding documents make it difficult to involve all affected parties, especially in the case of NSC directives. For activities that are part of the core responsibility of organizations represented

at the CCB, there are documented restrictions that forbid further dissemination of the directives without authority from the Chairman of the Joint Chiefs of Staff and/or the NSC itself.

(3) Discussion and way ahead. Mr. [redacted] suggested that the CCB should investigate the pros and cons of leveraging the oversight group of the DOD CIO National Leadership Command Capabilities (NLCC) Executive Management Board. The NLCC EMB oversees several active working groups that meet regularly, use an up-to-date SharePoint portal on the SIPRNET, and have participants from many of the same organizations that have a role in the DCL. This group could possibly provide a SIPRNET repository for the key DCL reference documents, and mighg help advocate for more appropriate guidelines on dissemination of NSC decisions and other restricted material. Mr. [redacted] from the DISA SNLC office presented a 2009 memorandum from the OASD(NII) office (predecessor of the DOD CIO office) directing DISA to engage the NLCC EMB in just such a manner. The DISA SNLC office will determine how and when to approach the NLCC EMB to establish a productive and interactive process. All parties recognized the need to update the CCB charter itself. The CIO/G6 office will circulate a draft update of the CCB charter by 29 June, with a request for detailed comments and responses from other organizations in a 45-day review period.

6. Implementation.

(1) Current status. An Information Systems Mission Order (IMSO) from US Army Information Systems Command (USAISC) (the predecessor to the US Army Network Enterprise Technology Command, NETCOM) covers the implementation in detail. A DCL Engineering Modernization Plan from ITA is likewise very thorough. Even so, these documents are now between 5 and 20 years old. Several other reference documents are on hand to guide the implementation roles of each organization. The ISEC office has proposed a particular method for updating the DCL network to an Internet Protocol (IP) configuration. The US and Russian sides have discussed this concept in general terms, and the US side will seek to present the proposal to the Russian side once it is developed further.

(2) Challenges. Various offices have different definitions and expectations for terms such as “sustainment,” “modernization,” and so on. In recent years, offices responsible for particular segments of the DCL system have made modifications without full agreement from other affected parties. Leaders in any one part of the effort cannot make the best decisions if they do not have an accurate view of activities in other parts of the network. With regard to the proposal for IP modernization, not all offices are fully aware of the details and implications.

(3) Discussion and way ahead. Mr. [redacted] presented a draft template for proposing and tracking modifications to components of the DCL. This template is at Enclosure 2. Mr. [redacted] will include this template within the updated CCB charter. Regarding the proposal for an overall IP upgrade, the ISEC office will begin to obtain hardware materials for this design, but the US side will conduct a more detailed review and finalize the plan before presenting it to our Russian counterparts.

7. Next CCB meeting. Mr. [redacted] from the 21st Signal Brigade recommended that the CCB should meet again after a 3-month period, on account of the level of information and potential recommendations that the group is likely to consider. Also, Mr. [redacted] offered to host the next CCB meeting at the 21st Signal Brigade headquarters at Fort Detrick, Maryland.

8. The point of contact for this document is Mr. [redacted], Army CIO/G6 office, (571) 256-8975, [redacted]@us.army.mil.

[redacted]
Chief, LandWarNet Network Integration Division
Army CIO/G6

DISTRIBUTION:

Army HQDA CIO/G6-AOI
Army HQDA G8-FDC
Army PM DCATS / PD SCS
Army 21st Signal Brigade
Army 302d Signal Battalion
Army Information Systems Engineering Command
Secretary of Defense Communications Office
Defense Information Systems Agency
National Security Agency
White House Communications Agency
State Department

Enclosures:
1. Attendance list
2. Proposed template for DCL system modifications

Configuration Control Board (CCB)
for the Direct Communications Link (DCL)

22 May 2012

Organization	CCB Membership*	Name	E-mail	Phone	Present
Army HQDA CIO/G6	CCB	[redacted]	[redacted]@mail.mil	(571) 256-8988	
Army HQDA CIO/G6		[redacted]	[redacted]@us.army.mil	(571) 256-8975	
Army HQDA CIO/G6		[redacted]	[redacted]@mail.mil	(571) 256-8962	
Army HQDA G8-FDC		[redacted]	[redacted]e@conus.army.mil	(703) 697-9065	
Army ITA	CCB	[redacted]	[redacted].civ@mail.mil	(703) 614-6597	
Army ITA		[redacted]	[redacted].civ@mail.mil	(703) 614-6604	
Army 21st Signal Brigade	CCB	[redacted]	[redacted]@mail.mil	(301) 619-6827	
Army 21st Signal Brigade		[redacted]	[redacted]@mail.mil	(301) 619-6784	
Army 21st Signal Brigade		[redacted]	[redacted].civ@mail.mil	(301) 619-6163	
Army 21st Signal Brigade		[redacted]	[redacted].civ@mail.mil	(301) 619-6150	
Army 302d Signal Battalion		[redacted]	[redacted]@mail.mil	(301) 619-3748	
Army PM DCATS / PD SCS	CCB	[redacted]	[redacted].civ@mail.mil	(703) 806-9100	
Army PM DCATS / PD SCS		[redacted]	[redacted].civ@mail.mil	(443) 395-9649	
Army PM DCATS / PD SCS		[redacted]	[redacted].civ@mail.mil	(703) 806-8442	
Army ISEC		[redacted]	[redacted].civ@mail.mil	(520) 533-0854	
Joint Staff J3/MOLINK	AC	[redacted]	[redacted]@js.pentagon.mil	(703) 697-9240	
WHCA	AC	[redacted]	[redacted]@whmo.mil	(202) 757-6719	
NSA		[redacted]	[redacted]@mcs.ncsc.mil	(410) 854-8092	
NSA		[redacted]	[redacted]@nsa.gov	(410) 854-1408	
SECDEF Communications Office		[redacted]	[redacted]@sd.mil	(703) 692-7006	
State Department	AC	[redacted]	[redacted]@state.gov	(202) 647-7779	
State Department		[redacted]	[redacted]@state.gov	(202) 647-7884	
DISA	AC	[redacted]	[redacted]civ@mail.mil	(301) 225-2912	

* *CCB: Direct member of Configuration Control Board*
AC: Advisory Committee

TAB V

(U) ANNEX C: BLUE TEAM/STRATEGIC VULNERABILITY ASSESSMENTS NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICES, CYBERSECURITY DIRECTORATE, MISSION READINESS, TERMS AND CONDITIONS

(U) Version 4.1
(U) 09 October 2019

(U) PURPOSE AND SCOPE

A. (U) The following service options and additional terms and conditions apply to Strategic Vulnerability Assessments (SVA) provided by the National Security Agency/Central Security Service's (NSA/CSS) Mission Readiness.
B. (U) Providing SVA services to the undersigned entity (Customer) is subject to the Customer agreeing and complying with the following additional terms and conditions, and requires the Customer to send Mission Readiness a completed and signed copy of this Annex.
C. (U) Section III contains a detailed description of Mission Readiness Blue Team SVA mission and methodology.

I. (U) BLUE TEAM SVA REQUIREMENTS

(U//FOUO) During an SVA, Mission Readiness Blue Team will access the Customer's network for the purpose of identifying vulnerabilities and improving the overall security posture of the network against adversarial threats, including both malicious insiders and external adversaries. The following core conditions and assumptions are essential to enabling the Blue Team to operate at maximum effectiveness. Constraints placed on any of the following will significantly impact the effectiveness of the SVA mission.

1. (U) Customer shall provide Blue Team with Customer network topologies and diagrams; system configuration documentation detailing internal and external network connections, enterprise-wide services, physical hardware, etc.; and numbers and types of physical and virtual hosts and devices. Technical details will be specified during subsequent technical scoping meetings.
2. (U) Customer shall provide Blue Team a list of domains, IP addresses, and/or subnets of hosts and devices considered in-scope for the SVA.
3. (U) Customer shall provide Blue Team operators the following privileged credentials:
    - Windows Domain Administrator credentials
    - Level 15 or Administrative Access to all infrastructure devices in-scope
    - Root or SUDO access to all UNIX hosts in-scope
    - Additional details about the privileged credentials can be found in Section IV.
4. (U) Customer shall provide Blue Team full network access via physical, virtual, console, etc. to the network, hosts, and devices to perform data collection including system logs, and applicable host files and configurations. Blue Team will utilize proprietary collection capabilities to obtain data by direct scanning, remote access or physical connection to hosts and devices. Blue Team will *not* modify host or device configurations.
5. (U) Customer shall provide Blue Team access to perform network traffic data collection. Network traffic collection may include sensor placement at *all* key nodes to optimize analysis. Blue Team will work with the Customer's network engineers to determine optimal placement of

sensors. In the event the network topology changes, or the Blue Team identifies coverage gaps, loss of collection quality, visibility, or connectivity, the Customer will provide timely, on-going support to adjust sensor placement and\or configurations to establish required network visibility. In addition, if a new key node is discovered or if the importance of the nodes changes with on-mission discovery, the Blue Team may require adjustment of sensor placement to ensure maximum visibility of critical system components.

6. (U) Customer shall provide Blue Team operators physical access, along with any credentials or badges to access Customer designated working space to conduct the SVA. When possible, the SVA should not require escorts in the Customer facility. If escorts are required, the Customer shall notify Mission Readiness of the requirement before the SVA and the Customer shall provide enough escorts for the entire SVA team. The Customer shall provide Blue Team operators adequate working space, physical connections to the network, adequate network throughput, and electrical power and connections.
7. (U) If the Blue Team is not couriering classified data back to NSA, upon completion of the SVA, the Customer shall provide Blue Team operators an approved data destruction mechanism at the classification level of the assessed network.
8. (U) Customer may provide, in writing, a list of IP addresses of hosts or devices that are considered conditional, not in-scope, or off-limits. This list must also provide justification for excluding these systems from the SVA.
9. (U) Customer may also provide, in writing, a list of high priority IP addresses that would be a prime target for adversaries (i.e., administrator systems or hosts, senior executive's hosts, centralized network management systems, mission critical systems, etc.) The list should include the IP address and reason for the high priority determination.

II. (U) Blue Team Overview

(U) Mission

(U) The National Security Agency's Blue Team is responsible for performing SVAs, Intrusion Detection Analysis, and Incident Response of Customer networks. The intent of an SVA is to identify vulnerabilities and improve the overall security posture of the network against adversarial threats, including both malicious insiders and external adversaries.

(U) The Blue Team conducts on-site missions. Blue Team SVAs utilize Mission Readiness Intelligence and Information Driven Operations (I2DO) methodology to guide Customer selection and to aid in the creation and adaptation of Blue Team tools, techniques and procedures. SVAs are focused on identifying vulnerabilities to improve the overall Customer network security posture. The IDA mission is performed in tandem with an SVA and aims to identify potential malicious activity or vulnerabilities that may have been exploited by an adversary. While on-site, Blue Team operators collaborate with the local network and system administrators to better understand the Customer mission as it relates to network security, requirements, and constraints. The Blue Team receives privileged credentials from the Customer and relies on cooperation with the Customer to collect data using Blue Team tools from the Customer network and hosts.

(U//FOUO) [redacted]

[redacted].

(U) Methodology

(U) During a SVA, Blue Team operators perform vulnerability and anomaly detection through data correlation and manual analysis, and are responsible for identifying systemic and unique vulnerabilities across the network. One of the most crucial steps to a successful Blue Team operation is verifying host integrity, which provides assurance to the operator that data collected from the host is complete, true, and trustworthy. Throughout the mission, Blue Team operators assess both the technical and non-technical aspects of hosts, devices, and the overall network. Some examples of technical findings include: verification of host integrity, checking centralized authorization implementations, cataloging of ageing or end-of-life hosts, and the implementation of security hardening guidelines. Non-technical findings include assessments of: the overall health and wellness of the network, the effectiveness of defense-in-depth strategies, and the existence and usage of user procedures and documentation.

(U//FOUO) [redacted].

(U//FOUO) [redacted].

(U//FOUO) [redacted].

(U) The Blue Team is not an accreditation team and does not approve or revoke network Authority to Operate (ATO). Blue Team SVAs are not intended to ensure Customer networks will pass certification and accreditation reviews, nor are they intended to replace or supplement a Customer's Security Operations Center (SOC). All Blue Team SVAs are performed with the intent to uncover vulnerabilities and improve the overall security of Customer networks, but no assessment can claim to identify all vulnerabilities existent on any given network.

III. (U) Mission Requirements

(U) Credentials

(U//FOUO) [redacted].

(U//FOUO) [redacted].

(U//FOUO) [redacted].

(U//FOUO)

Network Device Type	Type of Access Required
Windows Active Directory	[redacted]
Network Infrastructure Devices (routers, switches, firewalls, proxies, etc.)	[redacted]
UNIX and Linux Hosts	[redacted]
Call Manager	[redacted]
Unmanaged Devices (printers, APC, non-domain joined hosts, etc.)	[redacted]

Table 1 (U//FOUO) Blue Team SVA Privileged Account Requirements

(U//FOUO)

(U) Whitelisting

(U) Whitelisting may be required and is dependent upon the Customer network configuration. Blue Team may require whitelisting of accounts, IP addresses, hostnames, executables, paths, or ports.

(U//FOUO) [redacted]

- [redacted]

IV. U) Communication

(U) Customer Information Requests

(U) Keep Blue Team apprised of any planned changes, outages, or upgrades before, during, or immediately after the SVA.

(U) Advise Blue Team of any on-going investigations or security incidents. This communication ensures Blue Team does not delete or age-off any data that may be pertinent to the investigation.

(U) Provide Blue Team access to logical network diagrams prior to commencing operations on the Customer network.

(U) Provide reporting and troubleshooting Points of Contact (POCs) including out of band communication channels (e.g., name, position, phone number, e-mail/distribution list).

(U) Provide High Value Target List: A target or asset whose denial or loss of access would negatively impact Customer mission.

(U) Provide documentation and details of Cross Domain Solutions (CDS) within the network.

(U) Provide a list of known or Customer perceived threats and threat actors with supporting documentation.

(U) Mission Readiness Communication to the Customer

(U//FOUO) [redacted]

(U//FOUO) [redacted]

Defense Information Systems Agency (DISA)

(Customer)

Signature: [redacted] Digitally signed by: [redacted]
[illegible]

Name: [redacted]

Title: Risk Management Executive/Authorizing Official

Date: 29 March 2020

TAB W

Department of the Army
1st Personnel Command, Washington-Moscow Direct Communication Link (DCL), Detrick Earth Station
Fort Detrick, Maryland
Office of Special Counsel File Number DI-17-2168

List of Witnesses	**Reference & Title in Report**
[redacted] Civilian Executive Officer U.S. Army Signal Activity Fort Detrick, Maryland	Chief Executive Officer
Mr [redacted] Linguist U.S. Army Signal Activity Fort Detrick, Maryland	Whistleblower
[redacted] Defense Information System Agency (DISA IE) Director/Chief Senior National Leadership Communications Division Fort Meade, Maryland	DISA IE Director, SNLC Div
[redacted] Satellite Terminal Systems PdM Wideband Enterprise Satellite Systems (WESS) Program Executive Office – Electronic Information System (PEO-EIS) Fort Belvoir, Virginia	Sat Term Sys PdM
[redacted] Telecommunications Specialist U.S. Army Signal Activity Fort Detrick, Maryland	Telecommus Specialist
[redacted] Director Network & Space Integration Headquarters Department of the Army Chief Information Office (HQDA CIO/G6)	Dir, Network& Space Integr