


TAB E

PRIVACY ACT STATEMENT


The Privacy Act of 1974 prohibits any department or agency of the Federal Government from releasing and personal information about an individual without that individual's written permission.

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.



DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND
8826 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

ARCC-OPF

MEMORANDUM FOR RECORD

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

1. On 21 August 2019 I met with Mr. [REDACTED], Satellite Terminal Systems PdM Wideband Enterprise Satellite Systems (WESS). I advised him that I am the assigned investigating officer conducting an inquiry in to the alleged conduct that may constitute a violation of law, rule, or regulation, gross mismanagement, and substantial and specific danger to public safety. I read the privacy statement and reiterated at the end our interview that these proceedings were to remain undisclosed. As such, the following allegations were investigated.
2. Pertaining to allegation 1 - why, despite the requirement for a Configurations Control Board (CCB) in the 2008 Information Plan for the C-Band Satellite Transmit and Receive Systems Direct Communications Link Earth Station Mr. [REDACTED] is concerned that the lack of a CCB has created serious risks for the DES. He has reached out to HQDA CIO/G6, the assigned Chair of the CCB for assistance. A representative from the CIO/G6 was invited to the Quarterly Program Review at Fort Detrick from 4-5 September. No represented participated.
3. Pertaining to allegation 2 - why, since the 2015 reorganization and consolidation of Detrick Earth Station, has there not been a full review the Information Assurance Plan (IAP) under the Risk Management Framework established in 2014, Mr. [REDACTED] acknowledged that the DES requires a current IAP.
4. Pertaining to allegation 3 - why have there been security and operational deficiencies attributable to remote operations persist at the Detrick Earth Station, including poor security monitoring, that have left the facility vulnerable, Mr. [REDACTED] has no knowledge of this allegation.
5. Pertaining to allegation 4 - whether the lack of a fire suppression system required by the Information Assurance Plan and a lack of 24/7 personnel presence has led to security and operational deficiencies Mr. [REDACTED] has no knowledge of this allegation.

ARCC-OPF

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

6. Mr. [REDACTED] provided two briefings for review (enclosed at Tab G). The Senior National Leadership Communications (SNLC) Direct Communications Link (DCL) Modernization Project Brief, dated 14 August 2019. The SNLC Quarterly Program Review, dated 4-5 September 2019. The first briefing provides an overview of the approved modernization project to upgrade the antennas for the DES. Mr. Thrasher recommends in his correspondence that this project be halted in an effort to save taxpayer dollars. The second briefing provides recommendations to submit the RMF paperwork to the Defense Information Systems Agency (DISA) no later than 13 September 2019 (slide 3), and to reconvene the CCB on a quarterly basis (slide 11). It is noted that Mr. [REDACTED] was not aware of any of these allegations prior to being contacted the Investigating Officer (IO).

7. I concluded my interview with Mr. [REDACTED] at 1320 hours on 23 August 2019.

8. POC for this memorandum is the undersigned at 703-706-2558 or [REDACTED].civ@mail.mil.

[REDACTED]
GS 15
Investigating Officer

SWORN STATEMENT

For use of this form, see AR 190-46; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).
PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.
ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.
DISCLOSURE: Disclosure of your SSN and other information is voluntary.

1. LOCATION FT BELVOIR, BLDG 1456 PEO-EIS	2. DATE (YYYYMMDD) 2019 08 23	3. TIME 1320	4. FILE NUMBER
5. LAST NAME, FIRST NAME, MIDDLE NAME [REDACTED]	6. SSN DoDI	7. GRADE/STATUS GS13	
8. ORGANIZATION OR ADDRESS PEO-EIS, BLDG 1456, FORT BELVOIR			

9. I, [REDACTED], WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:
 "Why hasn't DISA established a CCB for the management of the Detrick Earth Station (DES)?"
 I was recently assigned to RDM WESS & have been working the acquisition portion of the SNLC since June. I have spent time w/ different SNLC stakeholders (ISEC, WH, DISA) - WE ARE ALL IN AGREEMENT THAT THE LACK OF CCB HAS CREATED SERIOUS RISK FOR THIS CRITICAL COMMUNICATIONS PROGRAM. FROM THE CHARTER & DIRECTIVES, CIO G6 SHOULD BE CREATING THE CCB w/ OTHER STAKE HOLDERS AS VOTING OR NON-VOTING MEMBERS. MYSELF & OTHER STAKEHOLDERS HAVE REACHED OUT TO CIO G6 FORMER AONS OFFICE TO GET PARTICIPATION IN AN UPCOMING QUARTERLY PROGRAM REVIEW (4-5 SEP (WED/THUR)) IN HOPES OF RESTARTING THE CCB EFFORTS. ~~FROM~~ ^{SEM} FROM THE SNLC MATERIALS THAT I HAVE READ - NONE OF IT POINTS TO DISA TO ESTABLISH AND RUN THE CCB.

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT [REDACTED]	PAGE 1 OF <u>3</u> PAGES
-------------	---	--------------------------

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF _____ TAKEN AT _____ DATED _____"

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF [REDACTED] TAKEN AT FT. BELVOIR DATED 23 AUG 19

9. STATEMENT (Continued)

"WHY HASN'T THERE BEEN A FULL REVIEW OF IAP/DIACAP OF THE DES"

I AM THE PROJECT LEAD + COR OF THE DCL (DIRECT COMMUNICATIONS LINK) DES @ FT DETRICK. ONE OF OUR TASKINGS HAS BEEN TO REVIEW THE RMF REQUIREMENTS AND ENSURE THAT THEY DONOT CREATE SCHEDULE/PERFORMANCE RISK FOR THIS \$11M MODERNIZATION EFFORT

(WE ARE REPLACING THE X2 ANTENNA'S, ADDING EQPT SHELTERS, & MODERNIZING THE MONITOR + CONTROL SYSTEM);

ADMITTEDLY, WE ARE HAVING DIFFICULTY IDENTIFYING BASIC INFO SUCH AS WHO ~~them~~ SHOULD BE THE DES/DCL AD BUT WE ARE WORKING WITH DISA, ISEC + 21ST SIG TO BEGIN THOSE DISCUSSIONS.

OUR INTENTIONS ARE TO COMPLETE THE RMF Paperwork, ASSESSMENT, ETC AND ENSURE THE NETWORK RISKS HAVE BEEN IDENTIFIED, ~~AND~~ ~~them~~ ASSESSED, MITIGATED, ETC.

NOTHING ELSE FOLLOWS

INITIALS OF PERSON MAKING STATEMENT

X [REDACTED]

PAGE 2 OF 3 PAGES

STATEMENT OF

TAKEN AT

FT BELVOIR

DATED

23 AUG 19

9. STATEMENT (Continued)

[The statement area is crossed out with a large X.]

AFFIDAVIT

I, [REDACTED], HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1, AND ENDS ON PAGE 3. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

[REDACTED]
(Signature of Person Making Statement)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 23 day of AUGUST, 2019 at FT BELVOIR, VA

ORGANIZATION OR ADDRESS

[REDACTED]
(Signature of Person Administering Oath)

ORGANIZATION OR ADDRESS

[REDACTED]
(Typed Name of Person Administering Oath)

Art. 136, UCMJ

(Authority To Administer Oaths)

INITIALS OF PERSON MAKING STATEMENT

PAGE 3 OF 3 PAGES



U.S. ARMY



Senior National Leadership Communications (SNLC) Direct Communications Link (DCL) Modernization

Project Brief

FT Detrick, 14 Aug 2019

21st Signal S3 Conference Room
Bridge # 301-909-7351 Access 27691730

John Myung
COR, Project Lead
Satellite Terminal Systems PdM WESS
Gov Cell 571-358-0622

PdMDCATS
Freedom Through Communications

PEIS

TAB I



Agenda



1. Project Scope
2. DCL Site Layout
3. Project Schedule
4. Near Term Coordination Items
5. Project Concurrence Memorandum (PCM)
6. Questions
7. Reference Slides



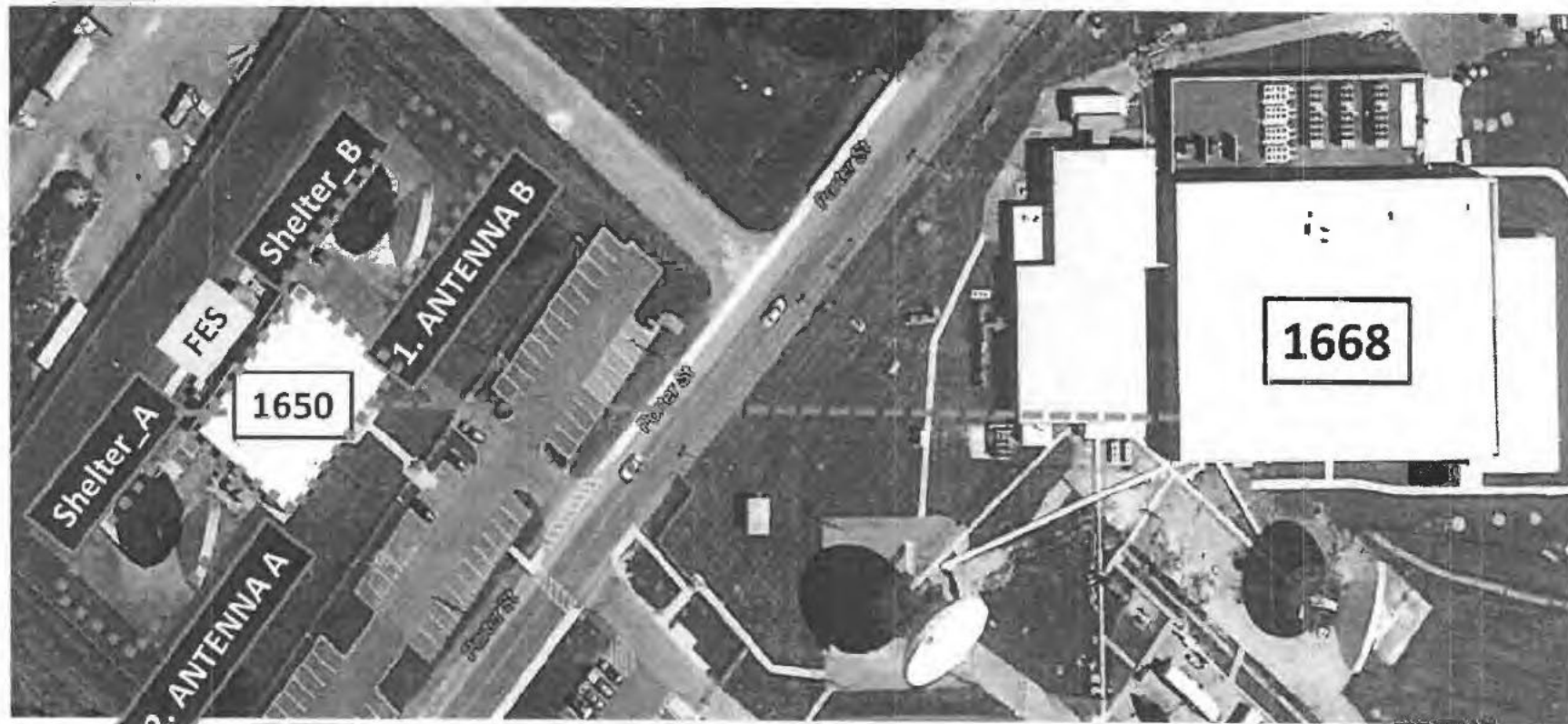
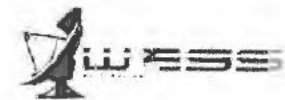
Project Scope



1. [TYAD] De-install Antenna's and platform preparation (site HVAC/power)
2. [CPI] Platform Load Frames, x2 Antenna's, x2 Shelters, Monitor & Control System (M&C), Interfacility Link (IFL)
3. [CPI/WESS] Test and Integration
4. [CPI] Provisional Acceptance Certification
5. [CPI/WESS] Training with Training Documentation
6. [CPI/WESS] Tech Manuals
7. Integrated Logistics Support
 - a) [CPI] 2-Year Warranty
 - b) [CPI] Return Material Authorization (RMA) instructions
 - c) [CPI/WESS] Spares and Special Tools List - PLL/Depot, TMDE, Expendable (common breakers/fuses)
 - d) [WESS] Life Cycle Sustainment (LCSP) & Disposition Plan



DCL Site Layout



XXXX = install/replace or modernize
FES = existing Foreign Equipment Shelter

DCL = Direct Communications Link

GTC = Global Telecommunications Center (Bldg 1668)

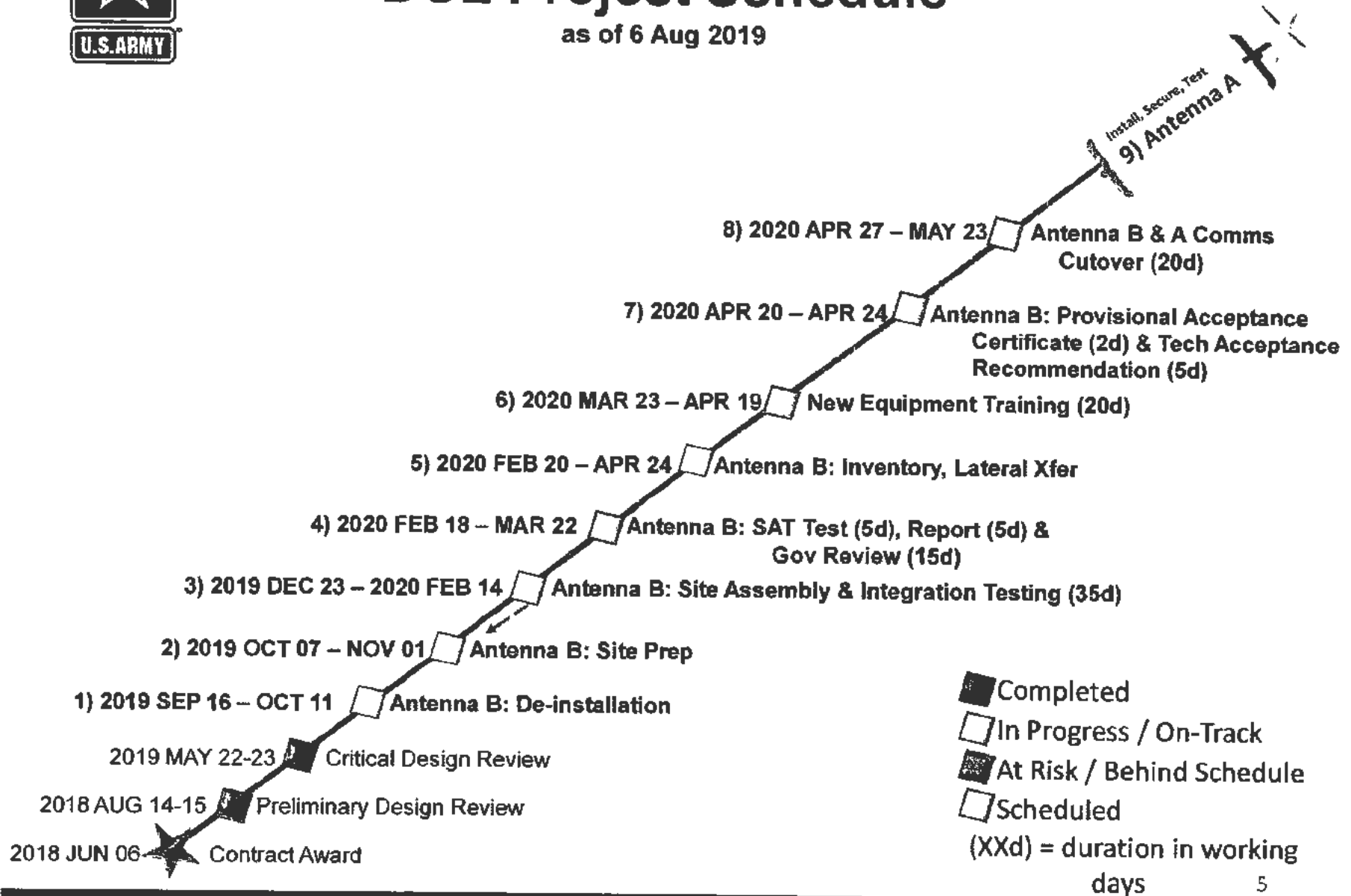
IFL = Inter-facility Link



DCL Project Schedule

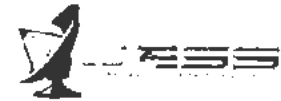
as of 6 Aug 2019

10) 2020 AUG 31
Contract Close





Near Term Coordination Items



1. De-install of Antenna B starting 16 Sep 2019 (user notifications, ASI's, etc)
2. Bldg 1650 Operations Floor
 - a) Completed by NLT 31 Aug 2020
 - b) Cabling and Power under the raised floor
 - c) Use of comms closet and patch panel
 - d) Fiber Implementation w/ USASA-Detrick
3. UPS requirement for FES, new DCL Antennas & Shelters:
 - a) PdM WESS UPS Requirement
 - b) FT Detrick Central Utility Power (CUP) implementation schedule
4. Logistics Coordination:
 - a) Shipping/Receiving – Laydown yard
 - b) Crane operations, Laydown yard, work areas, trash disposal
 - c) POC's on the ground during implementation & Project Updates
5. Risk Management Framework
 - a) Assessment for RU router and encryption
 - b) Validation of DAA, requirements and activities
6. SNLC Quarterly Program Review – Sep 4-5 (Weds & Thurs) @ FT Detrick



Project Concurrence Memorandum (PCM)



1. Discuss Project Scope & Responsibilities that are outside scope of contract.
2. Implement Lessons Learned/Best Practices from previous implementations.
3. PdM WESS submits to NETCOM => 21st Sig Bde => 302nd Sig Bn => USAASA



Questions





PdM WESS POC's



Mr. [REDACTED]
Contract Officer Representative, Project Lead
Satellite Terminal Systems
PEO EIS, PM DCATS, PdM WESS
DSN: (312) 656-8229
Commercial: (703) 806-8229
Government Cell: (571) 358-0622
[REDACTED].civ@mail.mil

Mr. [REDACTED]
Satellite Terminal Systems
PEO EIS, PM DCATS, PdM WESS
Office (443)395 9649
(Cell) (443) 655- 2695
[REDACTED].civ@mail.mil

Mr. [REDACTED]
Project Officer, Satellite Terminal Systems
PEO EIS, PM DCATS, PdM WESS
COM: (703) 806-4874
DSN: (312) 656-4874
Cell: (571) 355-1426
[REDACTED].civ@mail.mil

CPT [REDACTED]
CPT, SC/26A
Lead Engineer
US Army Information Systems Engineering Command
Transmission Systems Directorate (TSD)
Work - (520)454-1065
GC - (520)940-6027
[REDACTED].mit@mail.mil

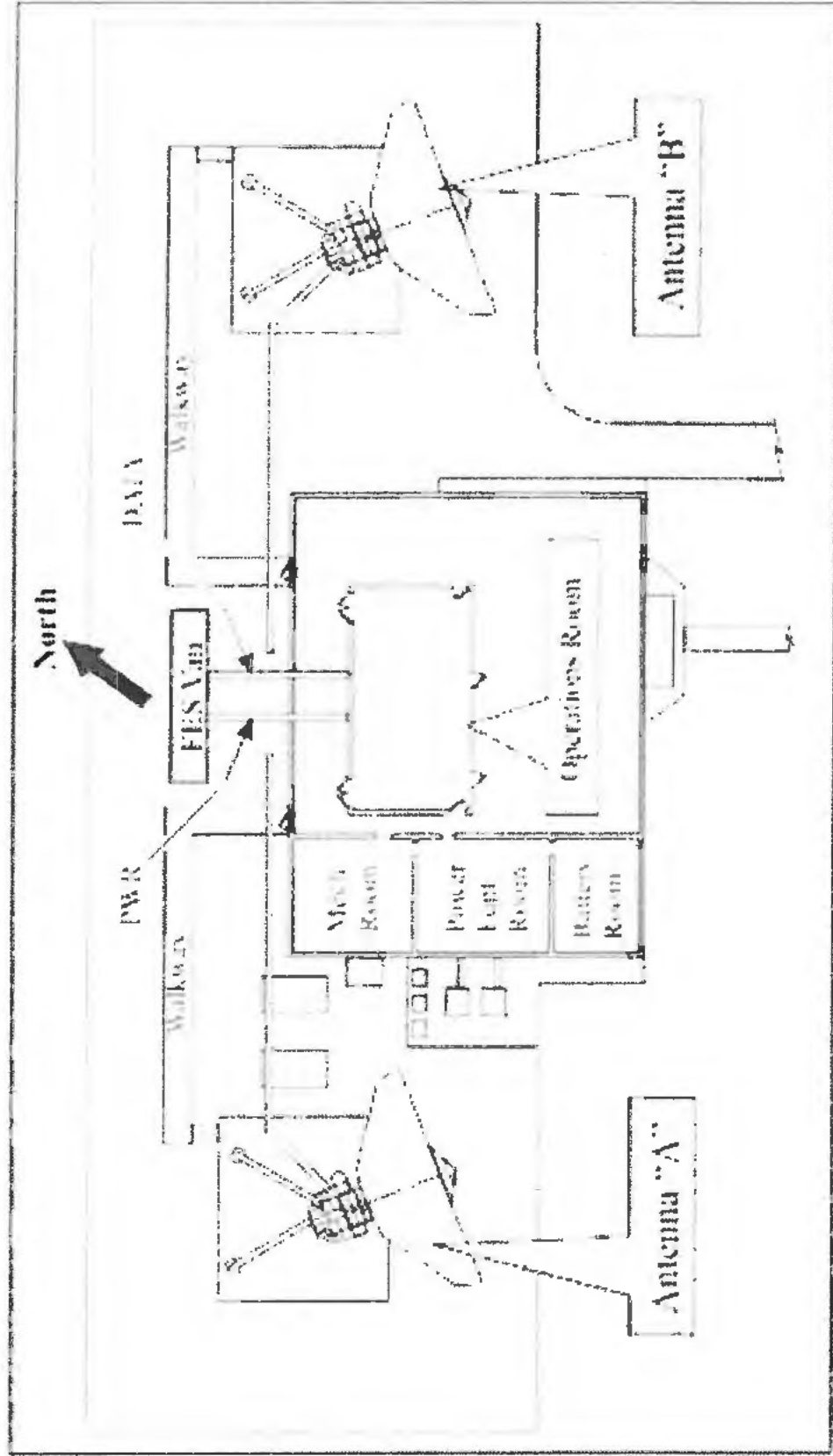
Mr. [REDACTED]
Production Engineering
Strategic Terminal Engineering Branch
Tobyhanna Army Depot (TYAD)
Desk (570) 615-8577
Cell: (570) 972-5992
[REDACTED].civ@mail.mil

Ms. [REDACTED]
Logistics Manager,
Satellite Terminal Systems
COM: (703) 806-8444
[REDACTED].civ@mail.mil

Mr. [REDACTED]
Project Coordinator
OFFICE: 703-806-8512
[REDACTED].ctr@mail.mil

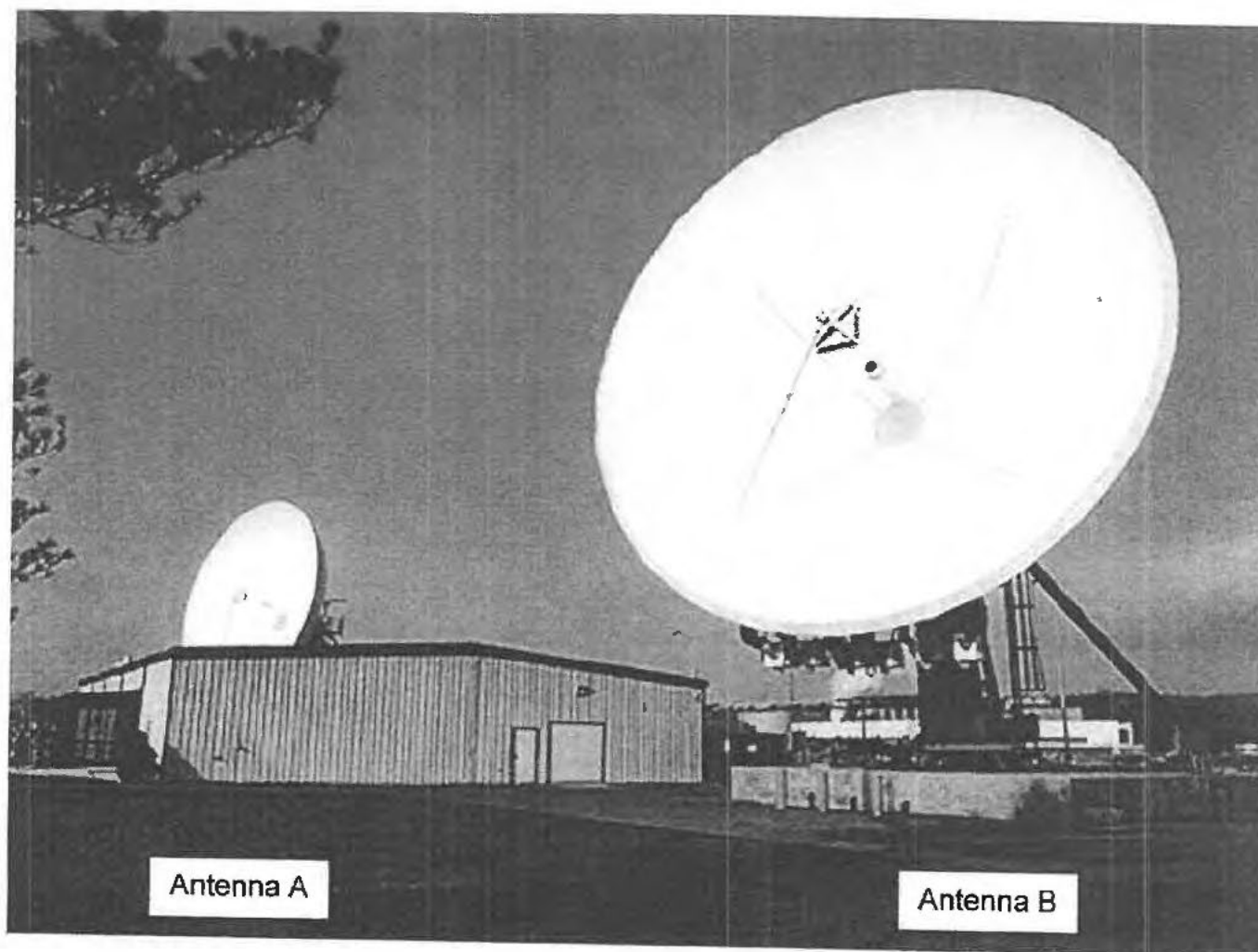
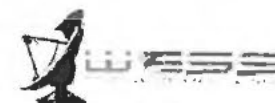


DCL Existing Site Plan w/ Foreign Equipment Shelter (FES)



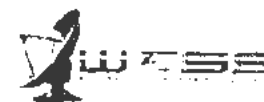


DCL Site Picture





Misc References & Artifacts



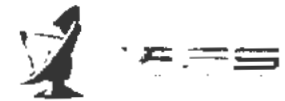
ISEC NETMAC n
MM



PCM vers
20190808



Acronyms



CPI - Communications & Power Industries LLC – formerly General Dynamics Mission Systems (GDMS)
CUP – Central Utility Power. FT Detrick DPW program to upgrade installation
DCL - Direct Communications Link (DCL)
DES - Fort Detrick Earth Station (DES)
FES – Foreign Equipment Shelter
GTC – Gateway Telecommunications Center (Bldg 1668)
IFL = Inter-facility Link
ISEC (USAISEC) – US Army Information Systems and Engineering Command
M&C – Monitor and Control (NETMAC)
NETMAC – Network Monitoring and Control System
PAC – Provisional Acceptance Certificate
PEO EIS / PM DCATS / PdM WESS / STS - Program Executive Officer, Enterprise Information Systems / Project Manager Defense Communications and Army Transmission Systems / Product Manager Wideband Enterprise Satellite Systems / Satellite Terminal Systems
SAT – Systems Acceptance Test
SNLC - Senior National Leadership Communications (SNLC)
TAR – Technical Acceptance Recommendation
TYAD – Tobyhanna Army Depot

TAB F

PRIVACY ACT STATEMENT

 The Privacy Act of 1974 prohibits any department or agency of the Federal Government from releasing and personal information about an individual without that individual's written permission.

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.



DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND
8825 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

ARCC-OPF

MEMORANDUM FOR RECORD

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

1. On 21 August 2019 I conducted a telephonic interview with Mr. [REDACTED] Telecommunications Specialist US Army Signal Activity-Fort Detrick, MD. I advised him that I am the assigned investigating officer conducting an inquiry in to the alleged conduct that may constitute a violation of law, rule, or regulation, gross mismanagement, and substantial and specific danger to public safety. I read the privacy statement and reiterated at the end our interview that these proceedings were to remain undisclosed. As such, the following allegations were investigated.

2. During the interview with Mr. [REDACTED] he offered the following detailed information.

a. Mr. [REDACTED] is a former Soldier and also served as a contractor for Honeywell International from 2006 to 2008. Honeywell was the Contractor providing personnel support to the DES until 2013. In 2013, Mr. [REDACTED] assumed his current role as Senior Telecommunications Specialist at the DES when the contract support converted to government personnel.

b. Pertaining to allegation 1- why, despite the requirement for a Configurations Control Board (CCB) in the 2008 Information Plan for the C-Band Satellite Transmit and Receive Systems Direct Communications Link Earth Station Mr. [REDACTED] is unaware of this requirement and offered no insight to this allegation.

c. Pertaining to allegation 2 - why, since the 2015 reorganization and consolidation of Detrick Earth Station, has there not been a full review the Information Assurance Plan (IAP) under the Risk Management Framework established in 2014, Mr. [REDACTED] is unaware of this requirement and offered no insight into this allegation.

d. Pertaining to allegation 3 - why have there been security and operational deficiencies attributable to remote operations persist at the Detrick Earth Station, including poor security monitoring, that have left the facility vulnerable, Mr. [REDACTED] cites an incident that occurred in 2015 (see email), where power was lost to the DES. The response time was hindered by the inability of personnel to

ARCC-OPF

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

access the turnstile gate because the power was out. At the time, [REDACTED] was in the building and was able to react to the situation.

e. Pertaining to allegation 4 - whether the lack of a fire suppression system required by the Information Assurance Plan and a lack of 24/7 personnel presence has led to security and operational deficiencies Mr. [REDACTED] is concerned that the mission does not receive the level of oversight it deserves. He acknowledges that a fire detection capability was added to the building but not fire suppression. He further stipulated that personnel protective equipment has been neglected. He alleges that the Standing Operating Procedures (SOPs), Concepts of Operations (CONOPS), and physical security plan have not been revised since Honeywell departed in 2013.

3. I concluded my interview with Mr. [REDACTED] this statement at 1630 hours on 29 August 2019.

4. POC for this memorandum is the undersigned at 703-706-2558 or [REDACTED]@mail.mil.

[REDACTED]

GS 15
Investigating Officer

CIV USARMY ARCYBER (USA)

TAB J

From: [REDACTED] CIV USARMY 21 SIG BDE (US)
Sent: Thursday, August 29, 2019 6:33 PM
To: [REDACTED] CIV USARMY ARCYBER (USA)
Subject: DES (UNCLASSIFIED)
Signed By: [REDACTED] civ@mail.mil

Classification: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

Ms. [REDACTED]

As a follow up to our conversation today, 29Aug2019, I am sending this email, at your request.

I am not aware of any CCB or Information Assurance Plan reviews that have taken place since the Honeywell contract ended for the DES.

Since the personnel were removed from the DES facility SOPs and Emergency Action Plans have largely been neglected, and equipment maintenance has suffered greatly.

The technicians hired to work in the DES had their position descriptions changed in 2014, and were re-assigned to work in the GTC (Army satcom facility), Tech Control Facility, and the Battalion SYSCON, in addition to the DES duties. The PD change along with the relocation of personnel has resulted in the operation of the DES becoming a minor part of daily operations, and not a focus of the attention that it deserves.

The relocation of personnel included addition of remote consoles to operate equipment that is in the DES facility (with no IA review), but it does not have the full capability that is available from front panel operations and has had a negative impact on response times to operational problems at the DES.

One incident occurred, and fortunately a Linguist was present in the DES at the time. The main circuit breaker tripped, leaving the communications equipment on UPS power. The power loss caused the gate to access the compound to become in-operational, so we were not able to access the facility. Because there was someone in the building, he was able to access the key to the sliding gate and open it for technicians to get into the facility and restore power.

There is no fire suppression system in the building, and fire detection was added when 24/7 personnel were removed.

Personnel Protective Equipment has also been neglected, specifically the fall prevention gear that has been expired for years. I have addressed this issue up the chain multiple times, and even took it up to the Brigade

Commander (Col [REDACTED]), who assured me that it would be replaced. As of yet, it still has not been replaced, the latest update is that they will wait until the new antennas are installed, and purchase new safety equipment at that time.

There are several people in the building on a regular basis now that have nothing to do with the operation or maintenance of the mission, since they have turned it into the company supply and administrative offices building.

There are plans to replace the operational equipment, with questions unanswered about certain capabilities that should have been addressed by a CCB before replacements were planned.

Please let me know if there is any additional information that I can provide to assist your investigation.


Respectfully,

[REDACTED]
Telecommunications Specialist
USASA-D
301-619-8220

CLASSIFICATION: UNCLASSIFIED

TAB G

PRIVACY ACT STATEMENT



The Privacy Act of 1974 prohibits any department or agency of the Federal Government from releasing and personal information about an individual without that individual's written permission.

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.



DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND
8826 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

ARCC-OPF

MEMORANDUM FOR RECORD

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

1. On 21 August 2019 I conducted a telephonic interview with COL [REDACTED] Director, Network & Space Integration, HQDA CIO/G6. COL [REDACTED] assumed his role in 2019. I advised him that I am the assigned investigating officer conducting an inquiry in to the alleged conduct that may constitute a violation of law, rule, or regulation, gross mismanage-ment, and substantial and specific danger to public safety. I read the privacy statement and reiterated at the end our interview that these proceedings were to remain undisclosed. As such, the following allegations were investigated.

2. Pertaining to allegation 1 - why, despite the requirement for a Configurations Control Board (CCB) in the 2006 Information Plan for the C-Band Satellite Transmit and Receive Systems Direct Communications Link Earth Station. COL [REDACTED] feedback confirmed that the current CIO/G6 leadership was unaware of their role to serve as the Chair of the Configuration Control Board (CCB). COL [REDACTED] is assigned as the Director, Network Systems and Services, HQDA CIO/G6, formerly Director for C4 Space and Networks, DISC4.

3. Pertaining to allegations 2, 3, and 4 COL [REDACTED] was unable to provide any pertinent information as a witness in this case.

a. Allegation 2 - why, since the 2015 reorganization and consolidation of Detrick Earth Station, has there not been a full review the Information Assurance Plan (IAP) under the Risk Management Framework (RMF) established in 2014.

b. Allegation 3 - why have there been security and operational deficiencies attributable to remote operations persist at the Detrick Earth Station, including poor security monitoring, that have left the facility vulnerable.

c. Allegation 4 - whether the lack of a fire suppression system required by the Information Assurance Plan and a lack of 24/7 personnel presence has led to security and operational deficiencies.

ARCC-OPF

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

4. I concluded my interview COL [REDACTED] at 1030 hours on 17 September 2019. COL [REDACTED] indicated that he would follow up on this requirement.

5. POC for this memorandum is the undersigned at 703-706-2558 or [REDACTED].civ@mail.mil.

[REDACTED]
GS 15
Investigating Officer

TAB H

TABL

21 March 2008

***Information Assurance Plan
for the
C-Band Satellite Transmit and Receive Systems
Direct Communications Link (DCL)
Earth Station***

FOR OFFICIAL USE ONLY

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

This page intentionally
left blank.

FOR OFFICIAL USE ONLY

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

Table of Contents

1. Purpose.....	1
2. Applicability	1
3. Scope.....	1
4. Applicable Documentation	1
5. Operational Environment	2
6. Earth Terminal Overview	2
7. Control, Monitor and Alarm	2
7.1 Site Equipment Alarms	3
8. DCL Earth Terminal Accreditation Not Required.....	3
9. Future Changes to the DCL.....	4
10. Physical Environment.....	5
11. Software Security Procedures.....	5
11.1 Unauthorized Software.....	5
12. DCL SATCOM terminal IAVM strategy	6
13. DIACAP Implementation Plan (DIP) Information	8
13.1 DIP Assigned IA Control Requirements	8
14. Warning Banner.....	16

1. Purpose

To describe the DCL terminal and the Information Assurance plans and procedures that are required for the DCL as a Satellite Communications (SATCOM) terminal that does not have an IT interconnect. The DCL meets the exemption requirement of DoDD 8500.1 paragraph 2.3 and will, therefore, be identified as DIACAP accreditation not required in the Army Portfolio Management Solution (APMS). This identification allows all parties involved to establish a cost effective solution of IA management for the DCL earth terminal as required in DoDD 8500.1 paragraph 4.2. This does not mean that DIACAP will not be performed at all; this plan plus the System Identification Profile and DIACAP Implementation Plan will be processed through a DIACAP process to obtain a letter of concurrence from the DAA at the Program Executive Office/Enterprise Information System (PEO/EIS).

2. Applicability

This plan will be used by certifying officials and users/maintainers of the DCL as the foundation for establishing the DCL terminal security boundaries and procedures.

3. Scope

All DOD military, civilian, and contractor personnel who access the DCL terminal.

All hardware and software fielded to the DCL terminal.

4. Applicable Documentation

Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance
06 July 2006

Department of Defense Directive 8500.1, Information Assurance (IA), October 24, 2002

Department of Defense Instruction 8500.2, Information Assurance (IA) Implementation, 6
February 2003

Department of Defense Instruction 8580.1, Information Assurance (IA) in the Defense
Acquisition System, 9 July 2004

Department of Defense Directive 8581.1E, Information Assurance (IA) Policy for Space
Systems Used by the Department of Defense, 21 June 2005

AR 25-2, Information Assurance

AR 190-13, The Army Physical Security Program.

AR 380-5, Department of the Army Information Security Program.

AR 380-67, Personnel Security Program.

AR 530-1, Operations Security (OPSEC)

Program Executive Office Enterprise Information Systems (PEO EIS) Policy Memorandum 06-01, PEO EIS Information Assurance (IA) Certification and Accreditation Program, 11 October 2005.

Memorandum for Record, Project Manager, Defense Communications and Army Transmission Systems (PM DCATS) Technical Management Division (TMD), dated 2 October 2007, Subject: The Listing of Satellite Communications Terminals as Accreditation Not Required On the Army Portfolio Management System (APMS)

5. Operational Environment

The Fort Detrick Direct Communications Link (DCL) earth terminal installed at Fort Detrick MD is for use by the U.S. Army and supports communications with the former Soviet Union countries located in three different countries. Each DCL terminal antenna is located in the antenna field next to the Earth Terminal Complex (ETC) building. The antenna field is secured by fencing. The entire DCL is operated within a physical controlled zone (PCZ) that provides all necessary physical protection commensurate with the classification level at which the DCL is being utilized. Access is controlled to the area of the location of the equipment, and a perimeter is established to restrict access. There are a total of 16 operators/maintainers that are authorized access to the DCL to provide 24 hrs/day 7 days a week operation. Access to the DCL will only be through those (highly trained) operators/maintainers. These personnel are dedicated to the DCL operations and maintenance and are cleared to (at a minimum) the secret level.

6. Earth Terminal Overview

The Fort Detrick Direct Communications Link (DCL) earth terminal is a dedicated satellite link station for special heads of state communications. The DCL terminal is a Radio Frequency (RF) satellite communications (C - band) terminal is only used to take the Intermediate Frequency (IF) signal from baseband equipment, upconvert it to RF (5.85-6.65 GHz frequency range), and amplify it for the antenna's uplink transmission to a satellite. At the satellite, the signal is downconverted and retransmitted for propagation at the downlink frequency (3.4 - 4.2 GHz frequency range), sent to earth where it is received by another (same) satellite earth terminal. The signal is then amplified and downconverted from RF and sent to the baseband equipment at the IF. At no time is data taken from the RF signal or applied to the RF signal as it is routed through the terminal. The DCL terminal is controlled via an isolated server based control system which is called the Control, Monitor and Alarm (CMA) system. At figure 1 is a block diagram of the DCL terminal. The Special Communications Network (SCN) is an isolated heads of state communications network. There are two (separate) DCL earth terminals; one for operation and one for backup for contingency purposes.

7. Control, Monitor and Alarm

The CMA only interfaces with the DCL radio equipment (except for alarm contact closures; see next paragraph). The baseband RF equipment located at the Fort Detrick DCL site has no interface to the CMA. A set of applications shall be installed into the DCL CMA for operation of the SATCOM equipment. The CMA consists of four Dell computers interconnected together. One acts as a server (with its corresponding hot spare) and one acts as a desktop computer (with

its corresponding hot spare). A list of the CMA equipment and their corresponding applications are listed below.

Item	Equipment	Application
1	Dell Optiplex 320 Desktop computer	Windows Server 2003 R2 Standard Edition Maxview
2	Dell Optiplex 320 Desktop computer	Windows Server 2003 R2 Standard Edition Maxview
3	Dell Optiplex 320 Desktop computer	Windows XP Professional Maxview
4	Dell Optiplex 320 Desktop computer	Windows XP Professional Maxview

7.1 Site Equipment Alarms

The CMA receives a contact closure from various pieces of equipment within the Earth Terminal Complex (ETC). These contact closures are interpreted by the CMA to provide alarm status to the operator. At the table below is a list of equipment providing alarm (contact closures) to the CMA.

Item	Equipment
1	Newbridge 3600 Mainstreet Bandwidth Manager (Multiplexer)
2	Cellwatch (UPS battery monitor)
3	Uninterrupted Power Source (UPS) (Exide Powerware Plus)
4	GPS (Truetime) timing for Newbridge

8. DCL Earth Terminal Accreditation Not Required

As gleaned from the system description above, the DCL earth terminal has the characteristics as identified in table one below. With no platform Information Technology (IT) interconnect, the DCL terminal does not require the regular DIACAP accreditation (reference paragraph 2.3 of 8500.2). However, as noted in the purpose (above) a DIACAP process to obtain a letter of concurrence from the IDAA shall be performed. Note that, in the future, if changes to the DCL earth terminal cause it to be interconnected with the Defense Information System Network (DISN), the DCL will go through DIACAP Certification and Accreditation.

Table 1. DCL earth terminal

Terminal Acronym	Contain CMA IT Component?	CMA Dedicated to Terminal?	Platform IT (CMA) Interconnect?
Fort Detrick Direct Communications Link (DCL) Terminal	Yes	Yes	No

9. Future Changes to the DCL

In the future there will be situations where some equipment will be replaced with form fit and function equipment because of technical upgrades or added to populate existing rack positions not initially utilized in the DCL. The purpose of the information below is to delineate those situations where making additions (or form fit and function replacements) of equipment in the DCL do not require IA to be readdressed for the DCL. This will result in the maintenance of a secure system whilst maintaining a cost effective C&A program for the DCL.

Equipment	Require DCL IA to be readdressed?	Rationale
RF transmitter	No	radio equipment not IA enabled
C band Low noise amplifier	No	radio equipment not IA enabled
C band Up/Down Converters	No	radio equipment not IA enabled
Antenna Control Unit	No	not IA enabled
Addition of C band Up/Down Converters	No	radio equipment not IA enabled
Addition of C band Low noise amplifier	No	radio equipment not IA enabled

10. Physical Environment

The local DCL Commander and Information Assurance Security Officer will protect the DCL through physical security measures in accordance with AR 190-13, Army Physical Security Program and FM 19-30.

An automatic emergency lighting system is installed at the DCL Earth Terminal Complex (ETC) that covers all areas necessary to maintain mission essential functions, to include emergency exits and evacuation routes.

The ETC has an Automatic humidity control that is installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation. Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

Critical power is provided to all DCL equipment via an UPS system that automatically controls the voltage and provides backup power if the commercial power is unavailable. The UPS units have Emergency cut-off switches that are activated by the operators to cut power to the SATCOM equipment.

11. Software Security Procedures

The local DCL Commander and Information Assurance Security Officer (IASO) will protect the DCL SATCOM terminal software through the use of software security procedures. What follows are measures that the site will take to ensure only authorized software loads are loaded onto the DCL SATCOM terminals.

11.1 Unauthorized Software

Only the delivered software (provided by PM DCATS) is authorized for use on DCL SATCOM terminals. Loading of additional software programs from any sources including enabling OS feature such as games, music download, Instant Messaging, Chat Box, etc, other than authorized revisions to the DCL SATCOM terminals software suite, is prohibited.

In order to maintain the configuration of the software, data files may not be transferred between DCL SATCOM terminals and other equipment at the site on removable media.

AR 710-2 requires original copies of all software, regardless of value, to be issued and accounted for through normal hand receipt procedures. In the case of the DCL SATCOM terminals, the Dell Optiplex 320s come from the manufacturer fully loaded with all software required for operation in the DCL SATCOM terminal. Unit Commanders and the local IASO will ensure that the Dell Optiplex 320s issued with each DCL CMA is properly accounted for and hand receipted. The local IASO will ensure that copyrighted software licensing restrictions are complied with in reference to the Dell Optiplex 320s. It is the responsibility of the local IASO to ensure the integrity of the DCL SATCOM terminals hardware (and by default software) suite.

12. DCL SATCOM terminal IAVM strategy

- a. The PM DCATS Post Deployment Software Support (PDSS) personnel shall review all Information Assurance Vulnerability Management (IAVM) correspondence for applicability to the Software baseline of the DCL SATCOM terminal.
- b. Implement and test applicable IAVMs correspondence in the Software Development Environment at Fort Monmouth.
- c. Rollup tested IAVMs into software version releases.
- d. Final releases of the software versions are tested at the Software Development Environment, Fort Monmouth prior to distribution to the DCL.

(

(

(

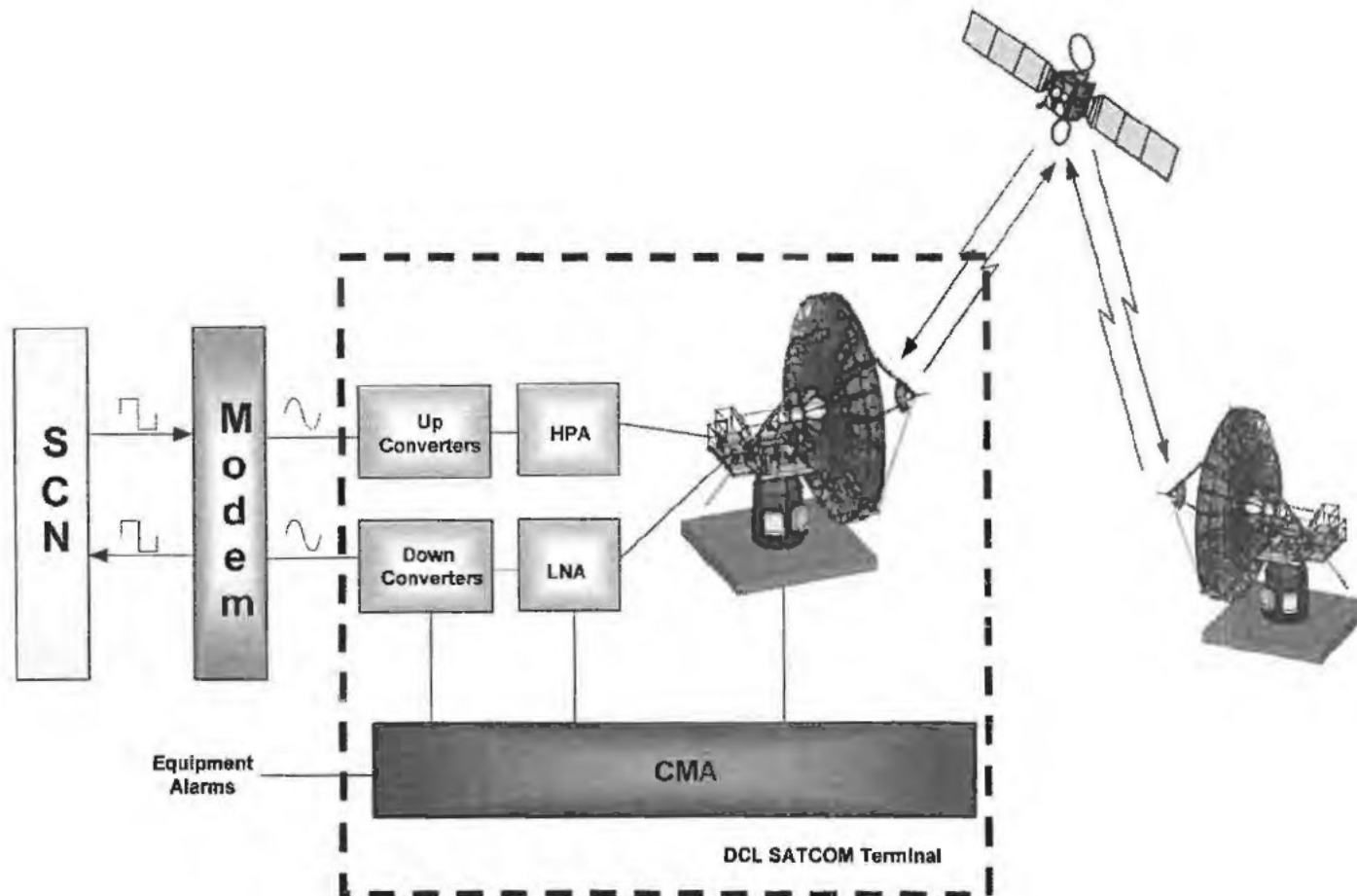


Figure 1. DCL Terminal (one of two identical systems shown)

13. DIACAP Implementation Plan (DIP) Information

In order to show clearly that the DCL meets all IA security category requirements of the DIP; the following information is provided (and keyed) to the DIP.

13.1 DIP Assigned IA Control Requirements

In the DIP a determination was found concerning the applicability or non applicability of certain IA controls. What follows is a table that goes step by step through each of the IA controls and provides informational discussions on applicability and rationale for the finding.

Assigned IA Control	Discussion
COAS-2	The DCL site consists of two DCL SATCOM terminals (DSTs); the main DST and An alternate DST that permits the restoration of all mission functions.
COBR-1	The DCL site consists of two DCL SATCOM terminals (DSTs); the main DST and An alternate DST that permits the restoration of all mission functions. Each DST is protected by physical and technical procedures to assure protection of the backup hardware, firmware, and software.
CODB-2	N/A - The DST does not contain data in the same sense that an Information System does, therefore data backup is not required. However, settings of the DST are located in each radio device and in the CMA. The DCL site consists of two DCL SATCOM terminals (DSTs); the main DST and An alternate DST that permits the restoration of all mission functions including the radio settings of the DST (ie; the radio settings of the main and backup are the same).
CODP-2	The DCL site consists of two DCL SATCOM terminals (DSTs); the main DST and An alternate DST that permits the restoration of all mission functions. A disaster plan exists that provides for the resumption of mission functions within 24 hours (or less) activation. (Disaster recovery procedures include mission recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)
COEB-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there are no enclave boundary defense requirements at the main or alternate site
COED-1	DST continuity of operations and disaster recovery plans are exercised annually by the site.
COEF-2	The DST's information transport function is identified for priority restoration planning along with all assets supporting the information transport function.
COMS-2	Maintenance support for the DST is available to respond 24 X 7 hours daily upon failure.
COPS-2	The DCL site UPS is configured to allow continuous, uninterrupted power to the DST. This includes backup generators.
COSP-1	Maintenance spares and spare parts for the DST can be obtained within 24 hours of failure.
COSW-1	Back-up copies of the CMA software (loaded onto Dell Optiplex 320s) are stored at the DCL and at PM DCATS, Fort Monmouth.
COTR-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network and because the DST is an information transport terminal; there is no nonsecure mode of operation for the DST.
DCAR-1	The DCL site conducts an annual IA review that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations of the DCL SATCOM equipment.
DCAS-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to acquire IA or IA-enabled IT products (that have been evaluated in accordance with NSA-approved processes) for the DST.

FOR OFFICIAL USE ONLY

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

DCBP-1	N/A - The DCL DST is an information transport system not connected to the DISN network. However, the DCL SATCOM terminal is designed for single sign-on user access.
DCCB-2	The DST is under the control of a chartered Configuration Control Board that meets regularly. The PM DCATS IASO is a member of the CCB.
DCCS-2	The technical manuals for the DST constitute the source for security implementation guidance for the few IA capabilities that the DST has.
DCCT-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network, no IA testing is required for the DST.
DCDS-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Acquisition or outsourcing of dedicated IA services is not required.
DCFA-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There are no external interfaces or information being exchanged by the DST.
DCHW-1	A current and comprehensive baseline configuration of the hardware of the DST (to include manufacturer, type, model and physical location) required to support operations is maintained by the Configuration Control Board (CCB) at PM DCATS. A backup copy of this inventory is stored in a container that is not collocated with the original.
DCID-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; No connection rules and requirements are applicable.
DCII-1	Changes to the DST (unless already addressed within this document) are assessed for IA and accreditation impact prior to implementation.
DCIT-1	N/A - Outsourced IT services are not being acquired as part of the DST project.
DCMC-1	N/A - Mobile code is not used in the DST.
DCNR-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; cryptography is not used in the DST. Note: all radio signals from the Site that are transported over the DST have been encrypted using NSA approved encryption devices.
DCPA-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; it has no user interface services (e.g., web services) that are accessed via the DISN. The DST also does not contain a data base or database management system.
DCPB-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; no discrete budget line item for Information Assurance is required. However, PM DCATS has an overall DST budget that is used to perform IA related efforts.
DCPD-1	N/A - Freeware (or shareware) is not used in the DST.
DCPP-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Ports, Protocols, and Services (to the DISN) are not used in the DST.
DCPR-1	PM DCATS has a configuration management (CM) process implemented for the DST that meets all requirements of DODI 8500.2 (DCPR-1).
DCSD-1	Even though the DST is a platform with no IT interconnect to the DISN network; appointments to required IA roles, e.g., DAA and IAM/IAO, are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. The site also has a System Security Plan established that describes the technical, administrative, and procedures and policies that govern the DST, and identifies all personnel and specific requirements and objectives (e.g., requirements for system redundancy or emergency response).
DCSL-1	Only authorized system administrators and users can update the DST software package. Only authorized software releases from PM DCATS are loaded onto the DST. This process protects the DST applications from the introduction of unauthorized code.
DCSP-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; The security support structure of the entire DST is isolation from the DISN.
DCSQ-1	N/A - The DST utilizes only approved COTS applications.
DCSR-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network and the DST is an information transport device (with no access to the information riding on the radio signal), IA-enabled products are not required for use in the DST.
DCSS-2	N/A - The DST utilizes only approved COTS applications.
DCSW-1	A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support the DST operations is maintained by the PM DCATS CCB. A backup copy of the inventory is stored in

**Information System Security Policy for the
Fort Detrick DCL Earth Terminal**

	a fire-rated container or otherwise not collocated with the original.
EBBD-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Boundary defense mechanisms are not required.
EBCR-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to follow DoD connection rules or approval processes.
EBPW-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There are no connections between the DST and the Internet or other public or commercial wide area networks.
EBRP-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There is no remote access to the DST.
EBRU-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There is no remote access to the DST.
EBVC-1	N/A - Because the DST is a platform with no IT Interconnect to the DISN network; the DST does not require VPN traffic or intrusion detection systems (IDS).
ECAD-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; The DST does not receive or transmit email. Therefore there are no email addresses, display names or automated signature blocks to label as part of DST operation.
ECAN-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; The DST does not have the capability for outside access to it.
ECAR-2	N/A - Note: due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; there is no requirement for individual logins to the DST for each operator/maintainer. Furthermore, because the DST is a platform with no IT interconnect to the DISN network there are no network security files or access ports. However, there is an audit record of the DST and it includes: Record of change(s) to system, Date and time of the change event, Type of change event and fault status information concerning the radio equipment.
ECAT-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network; the DST administrator or user cannot be on-line. However, an audit trail is maintained on the DST for use as needed to support IA investigations concerning the DST.
ECCD-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no access to the DST (accept for local access). However, an audit trail is maintained on the DST for use as needed to support IA investigations concerning the DST. Also, local logon to the DST shall be controlled via password access by authorized administrators and users located at the DST.
ECCR-1	N/A - There is no requirement to encrypt stored information that resides in the DST CMA.
ECCT-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; The DST does not transmit or receive data (it transmits and receives radio signals). However, at the DCL ETC; all data that is placed onto a radio signal for the DST to transport is encrypted using NSA approved cryptography.
ECDC-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network and is not a Transaction-based systems; this security category does not apply.
ECIC-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; The DST does not connect to other DoD information systems.
ECID-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Host-based intrusion detection systems are not required.
ECIM-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There is no Instant messaging traffic to/from the DST.
ECLO-1	N/A - Note: due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; there is no requirement for individual logins to the DST for each operator/maintainer.
ECLP-1	N/A - Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; there is no requirement for individual logins to the DST for each operator/maintainer.
ECML-1	For the DST, all CMA displays shall comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels on the CMA displays clearly reflect the sensitivity level of the information displayed on them.
ECMT-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Conformance testing that includes periodic, unannounced, in-depth monitoring and provides

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

	for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is possible.
ECND-2	Because the DST is a platform with no IT interconnect to the DISN network; The device control program consists of: instructions for restart of the CMA and maintenance documentation for the CMA.
ECNK-1	N/A – 1. Because the DST is a platform with no IT interconnect to the DISN network and 2. the DST (as a transport device) is not required to provide any encryption for the information riding on the radio signal it is transmitting (receiving) this is done before (after) it reaches (leaves) the DST.
ECPA-1	N/A – Due to the physical security capabilities and requirements of the DCL site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; there is no requirement for individual logins or role-based access schemes to the DST for each operator/maintainer.
ECPC-2	N/A – There are no Application programmers (that would change production code and/or data) that work on the DST. All software applications that reside on the DST are Commercial Off the Shelf (COTS).
ECRC-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to revoke authorizations to the information contained within an object prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. There is also no requirement for an object that has been released back to the system; for it to contain no information, including encrypted representations of information, produced by a prior subject's actions.
ECRG-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network; There is no access to the CMA from outside the DST that would be included into an audit record. However, an audit record does exist concerning local access to the CMA and is available for review.
ECRR-1	N/A - The DST does not contain sources and methods intelligence (SAMI). However, an audit record does exist concerning local access to the CMA and is available for review.
ECSC-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network and the CMA does not function as an enclave; DoD security configuration or implementation guides are not applicable.
ECSD-2	For the DST there is no software development, all software is COTS. Only authorized software packages from PM DCATS are loaded onto the DST CMA (by authorized personnel).
ECTB-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network; There is no access to the CMA from outside the DST that would be included into an audit record. However, an audit record does exist concerning local access to the CMA and is available for review. They are not backed up to a different system or media.
ECTC-1	N/A – The DST is not required to protect against TEMPEST related compromising emanations.
ECTM-2	N/A – Because the DST is a platform with no IT interconnect to the DISN network; there are no incoming and outgoing files that would need parity checks and cyclic redundancy checks (CRCs). For the DST there is no transmitted information (including labels and security parameters) and no communication sessions that may be hijacked.
ECTP-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network; There is no access to the CMA from outside the DST that would be included into an audit record. However, an audit record does exist concerning local access to the CMA and is available for review. The content of this audit trail is protected against unauthorized access by the password protection scheme on the CMA.
ECVI-1	N/A – Because the DST is a platform with no IT interconnect to the DISN network; There is no Voice over Internet Protocol (VoIP) traffic associated with the DST.
ECVP-1	N/A – Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; no virus protection is required at this time. Reference para 11.1 above.
ECWM-1	Upon use of the DST CMA, all users shall be warned that they are utilizing a Government information transport system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

**Information System Security Policy for the
Fort Detrick DCL Earth Terminal**

	Refer to para 14 below.
ECWN-1	N/A – The DST has no Wireless computing or networking capabilities at all.
IAAC-1	N/A – Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; there is no requirement for individual user accounts.
IAGA-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Group authenticators for network access is not required.
IAIA-2	N/A – Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; the DST does not require the presentation of an individual identifier (e.g., a unique token or user login ID) and password.
IAKM-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network; cryptography is not used in the DST. Therefore, cryptographic Keys are not required. Note: all radio signals from the Site that are transported over the DST have been encrypted using NSA approved encryption devices.
IATS-2	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Identification and authentication using the DoD PKI Class 3 (or 4) certificate is not required for users or administrators.
PECF-2	At the DCL ETC; only authorized personnel with a need-to-know are granted physical access to the DCL ETC.
PECS-1	At the DCL ETC; all documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C3I) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives."
PEDI-1	At the DCL ETC; devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.
PEEL-2	An automatic emergency lighting system is installed in the building that houses the DST. This lighting system covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.
PEFD-2	The DST Earth Terminal Complex (ETC) has two pull boxes that sound an alarm in the building and at the local (on base) fire department.
PEFI-1	The DST ETC undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.
PEFS-2	The DST ETC has two pull boxes that sound an alarm in the building and at the local (on base) fire department. There are also fire extinguishers on site.
PEHC-2	Automatic humidity controls are installed into the DST ETC to prevent humidity fluctuations potentially harmful to personnel or equipment operation.
PEMS-1	The UPS units have Emergency cut-off switches that are activated by the operators to cut power to the SATCOM equipment; they are labeled and protected by a cover to prevent accidental shut-off.
PEPF-1	At the DCL ETC; every physical access point to the DST is controlled during working hours; work hours are 24 X 7.
PEPS-1	At the DCL ETC; A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate the DCL ETC.
PESL-1	N/A – For mission purposes, the DST CMA screen(s) must be operational and viewable at all times.
PESP-1	At the DCL ETC; procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the DCL ETC.
PESS-1	At the DCL ETC; Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.
PETC-2	Automatic temperature controls are installed at the DST ETC to prevent temperature fluctuations potentially harmful to personnel or equipment operation.
PETN-1	Employees DST ETC receive initial and periodic training in the operation of environmental controls.
PEVC-1	At the DCL ETC; Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the DCL ETC.

**Information System Security Policy for the
Fort Detrick DCL Earth Terminal**

PEVR-1	Critical power is provided to the DST equipment via an UPS system that automatically controls the voltage and provides backup power if the commercial power is unavailable.
PRAS-1	At the DCL ETC; Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.
PRMP-1	At the DCL ETC; Maintenance is performed only by authorized personnel. The process for determining authorization and the list of authorized maintenance personnel is documented.
PRNK-1	At the DCL ETC; Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the site security officer.
PRRB-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there are no rules, responsibilities or expected behavior that describe the IA operations of the DST as it "connects" to the DISN (as an information system would).
PRTN-1	At the DCL ETC; A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA related plans such as incident response, configuration management and COOP or disaster recovery.
VIIR-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to establish a Computer Network Defense (CND) Service Provider (in accordance with DoD Instruction O-8530.2).
VIVM-1	Reference the "DCL SATCOM terminal IAVM strategy" paragraph above.
AR 25-2, 4-03	At the DCL ETC; A program is implemented to ensure that all personnel appointed to an IA position receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA related plans such as incident response, configuration management and COOP or disaster recovery.
AR 25-2, 4-05.a	At the DCL ETC; In addition to the prohibited activities listed in AR 25-1, the following activities are specifically prohibited by any authorized user on the DST: (1) Use of the DST for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes. (2) Installation of software, configuration of the DST, or connecting the DST to a distributed computer environment (DCE), for example the SETI project or the human genome research programs. (3) Modification of the DST or the DST software, use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software. (4) Physical relocation or changes to the configuration of the DST equipment. (5) Installation of non-Government-owned computing systems or devices without prior authorization of the appointed DAA including but not limited to USB devices, external media, personal or contractor-owned laptops, and MCDs. (6) Release, disclose, transfer, possess, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval. (7) Sharing personal accounts and authenticators (passwords or PINs) with any unauthorized individual. (8) Disabling or removing security or protective software and other mechanisms and their associated logs from the DST.
AR 25-2, 4-05.c(13)	At the DCL ETC; appropriate IA (for example, SA/NA) personnel shall have their accesses reinstated only after they have verified the reason for failed log-on attempts and have confirmed the access-holder's identity.
AR 25-2, 4-05.c(17)	At the DCL ETC; an access auditing and the protection of physical access control events (for example, card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts has been established.
AR 25-2, 4-05.d(4)	N/A - Because the DST is a platform with no IT interconnect to the DISN network; There is no remote access ability.
AR 25-2, 4-05.e	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there are no remote access servers.
AR 25-2, 4-05.j(5)	N/A - Because the DST is a platform with no IT interconnect to the DISN network; only trusted operators/maintainers have access to the DSTs information. The DST only contains a small

**Information System Security Policy for the
Fort Detrick DCL Earth Terminal**

	cadre of information required to operate the satellite radio.
AR 25-2, 4-05.k	The C&A package will be available to the DST IASO for the life of the DST. This C&A package will include the System Identification Profile (SIP), DIACAP Implementation Plan (DIP) and the IA Plan.
AR 25-2, 4-05.l	N/A - Because the DST is a platform with no IT interconnect to the DISN network; no security-related COTS hardware, firmware, and/or software components are required for the DST's protection.
AR 25-2, 4-05.q	N/A - Because the DST is a platform with no IT interconnect to the DISN network; no filtering policies to block ingress and egress services, content, sources, destinations, ports, and protocols are required.
AR 25-2, 4-05.t	N/A - because the DST is not an office automation product; there are no user files to be accessed during an absence of the user.
AR 25-2, 4-06.d	All software used on the DST is fully licensed.
AR 25-2, 4-06.f	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to "connect it" to an operational network.
AR 25-2, 4-08.b	N/A - Because the DST is an information transport system not an information-based system there is no requirement to implement software security solutions throughout the life cycle of the DST.
AR 25-2, 4-12.a	N/A - Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; there is no requirement for single sign on access to the DST.
AR 25-2, 4-13.b	N/A - Because the DST is a platform with no IT interconnect to the DISN network; the DST has no network vulnerabilities.
AR 25-2, 4-14	All personnel with access to the DST shall have at the minimum a secret clearance.
AR 25-2, 4-14.b (1)	N/A - Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; there is no requirement for individual user accounts that would require the principles of separation of duties and "least privilege" access.
AR 25-2, 4-15	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there are no email designation requirements. Foreign nationals are not allowed into the DCL ETC unless escorted.
AR 25-2, 4-16	At the DCL ETC; All equipment and facilities will be operated and secured where applicable per the DCID 6/3, AR 380-5, this regulation, or Joint DODIIS Cryptologic SCI Information Systems Security Standards (JDCSISSS). All DCL ETC personnel will mark, ship, store, process, and transmit classified or sensitive information in accordance with AR 380-5.
AR 25-2, 4-19	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there are no requirements for a cross domain solution.
AR 25-2, 4-20.b	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no logical access to the DST (only physical local access). Local logon to the DST shall be controlled via password access by authorized administrators and users located at the DST. Physical access to the DST will only be provided to individuals who can meet access requirements.
AR 25-2, 4-20.c	N/A - Because the DST is a platform with no IT interconnect to the DISN network and because the DST is a radio transport device; all information riding on the radio signal has already been encrypted by approved devices before it reaches the DST, the DST does not provide internet or NIPRNET access or contain internet modems.
AR 25-2, 4-20.d(6)	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no capability for the DST to provide Virtual Private Network (VPN) services.
AR 25-2, 4-20.d(7)	N/A - The DST does not have a "Storage area configuration" requirement or capability.
AR 25-2, 4-20.f	N/A - The DST does not have an "email" requirement or capability.

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

AR 25-2, 4-20.g	N/A - The DST does not have an "Internet" requirement or capability.
AR 25-2, 4-20.i	N/A - Due to the physical security capabilities and requirements of the site and that all operators/maintainers that have access to the site are authorized to operate/maintain the DST; and because the DST is a platform with no IT interconnect to the DISN network; no IA security software is required at this time.
AR 25-2, 4-20.j	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Networking security tools are not required.
AR 25-2, 4-20.k	N/A - The DST is a platform with no IT interconnect to the DISN network, it is not a tactical system; the DST is a radio transport device and does not include "features normally associated with an information system."
AR 25-2, 4-22	N/A - Because the DST is a platform with no IT interconnect to the DISN network; there is no requirement to report unusual or obvious incidents or occurrence to the theater RCERT. However, unusual or obvious incidents or occurrences that occur at the DCL ETC will be reported to the appropriate local authorities at Fort Detrick.
AR 25-2, 4-23	N/A - Because the DST is a platform with no IT interconnect to the DISN network; AR 25-2, 4-23 does not apply because there is no network access.
AR 25-2, 4-29	Portable electronic devices (PEDs) are prohibited from entering the DCL ETC.
AR 25-2, 4-30	N/A - The DCL ETC and/or the DST does not contain any wireless local area networks.
AR 25-2, 4-31	Employee-owned information systems (EOISs) are prohibited from entering the DCL ETC. There is no remote access to the DST.
AR 25-2, 4-32.c	Only cleared and technically qualified personnel are authorized to inspect equipment before equipment removal from the DCL ETC.
AR 25-2, 4-32.d	N/A - The DST does not contain any peripheral devices.
AR 25-2, 6-1	N/A - Because the DST is a platform with no IT interconnect to the DISN network; cryptography is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-1.a	N/A - Because the DST is a platform with no IT interconnect to the DISN network; cryptography is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-1.b	N/A - Because the DST is a platform with no IT interconnect to the DISN network; cryptography is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-1.c	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Cryptography (including FIPS 46-2 DES) is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-1.d	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Cryptography (including AES) is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-4(a-d)	N/A - Because the DST is a platform with no IT interconnect to the DISN network; Cryptography is not used in the DST. Note: all radio signals from the Site that are transported over the DST have already been encrypted using NSA approved encryption devices.
AR 25-2, 6-5	a. At the DCL ETC all personnel are prohibited from using Government-owned receiving, transmitting, recording, and amplification telecommunications equipment in restricted areas; such as classified work areas or mission essential vulnerable areas (MEVAs). b. At the DCL ETC all personnel will use NSA or CIO/G-8 provided secure telephones to discuss classified information telephonically. c. At the DCL ETC all personnel are prohibited from possessing or using any

Information System Security Policy for the
Fort Detrick DCL Earth Terminal

	privately owned PED (for example, cell phones, TWED) within the confines of classified, restricted, or open storage areas designated by the commander.
AR 380-5 2-18.a	A Security classification guides is in place that meets the requirements of AR 380-5 2-18.a. It is DCA circular 310-70-14, dated 1979 (confidential)
AR 380-5 4-16, 17	N/A – The DST does not generate any documentation that may require particular markings.
AR 380-5 6-19	N/A – The DST does not contain Information processing equipment as described in AR 380-5 6-19.
AR 380-5 APP E-3	N/A – Because the DST is a platform with no IT interconnect to the DISN network; the DST does not have the capability to process emails.
AR 380-5 APP E-8	N/A – Because the DST is a platform with no IT interconnect to the DISN network; the DST does not have web sites nor does it access web sites.

14. Warning Banner

The following warning will be placed next to all DST CMA display screens.

ATTENTION

THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING SBU INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING ENSURING THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

TAB I



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000
28 JUL 2000

TAB M

MEMORANDUM FOR SECRETARY OF THE ARMY

SUBJECT: Designation of the 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).


References: a. Memorandum, Office of the Under Secretary of Defense (C3I), March 14, 1984,
Subject: Upgrades to the USA/USSR Direct Communications Link (DCL)-(U)

b. Memorandum, Office of the Assistant Secretary of Defense (C3I), April 12, 1993,
Subject: Establishment of a Continuous Communications Link (CCL) with the Republic of Belarus, and Government-to-Government Communications Links (GGCL) with the Republic of Ukraine and Kazakhstan (U)

The Army remains the Lead Military Department (LMD) for the Direct Communications Link (DCL), the Continuous Communications Link (CCL) and the Government-to-Government Communications Links (GGCLs), per references.

As designated LMD, the Army will incur the life cycle management, procurement, installation, operation, training, maintenance and supply support responsibilities, as well as, the Planning, Programming and Budgeting System (PPBS) responsibilities.

In order to continue to maintain the DCL, CCL, and GGCL programs, an individual Program Element (PE) managed at HQ DA must be established. The designation as LMD for the DCL/CCL/GGCL may be used as justification to pursue the establishment of a distinct PE and subsequently establish necessary and appropriate Program Objective Memorandum (POM) funding. This action will ensure the institutionalization of the funding required to manage and modernize the DCL, CCL, and GGCL equipment and networks.


for R. J. Wijas
Director, Communications,
Command and Control (C3)



TAB J

UNCLASSIFIED

TAB N

CONFIGURATION CONTROL BOARD (CCB)

CHARTER

AUTHORITY

National Security Directive - 186 (NSD-186) provides overall guidance for continuation of the Direct Communications Link (DCL) program for the United States. This document, signed by President Ronald Reagan in November 1985, assigned Executive Agency for the National Communications System to the Secretary of Defense (SECDEF). SECDEF responsibilities under this directive include funding and implementation of the DCL program.

Deputy Under Secretary of Defense for Command, Control, Communications and Intelligence (DUSD/C3I) Memorandum, dated 14 March 1984, assigned life cycle support responsibility for the DCL program to the Department of the Army. The mission includes configuration control (hardware and software), funding, procurement, site survey, and associated engineering and installation of the U.S. portion of the DCL program.

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. In March 1992, DUSD-C3I assigned the Army the similar support responsibilities for the Continuous Communications Link (CCL) and Government-to-Government (GGCL) programs.

The Standing Sub-Committee for Upgrades (SSU) is the SECDEF body, authorized by the President, to set technical parameters and establish overall milestone schedules for upgrading the DCL system consistent with U.S./Russian agreements and national Security Policy. The SSU assigns engineering and procurement responsibilities and tracks milestone accomplishments. According to NSD-186, the SECDEF establishes the membership of the SSU.

UNCLASSIFIED

Army Regulation (AR) 25-1, The Army Information Resources Management Program, dated 25 March 1997, directs the Director of Information Systems for Command, Control, Communications and Computers (DISC4) to exercise configuration control over Army information systems and other DOD systems for which the Army has been given responsibility, including the DCL program. The DISC4 exercises management of the DCL program through a body called the Configuration Control Board (CCB), and establishes the position of Chairman of this body. A CCB is the regulatory body for controlling and evaluating software, hardware, and operational changes to the DCL system as prescribed in the Configuration Management (CM) Plan for the DCL program.

The relationship and membership of both the SSU and CCB are depicted at Figure 1.

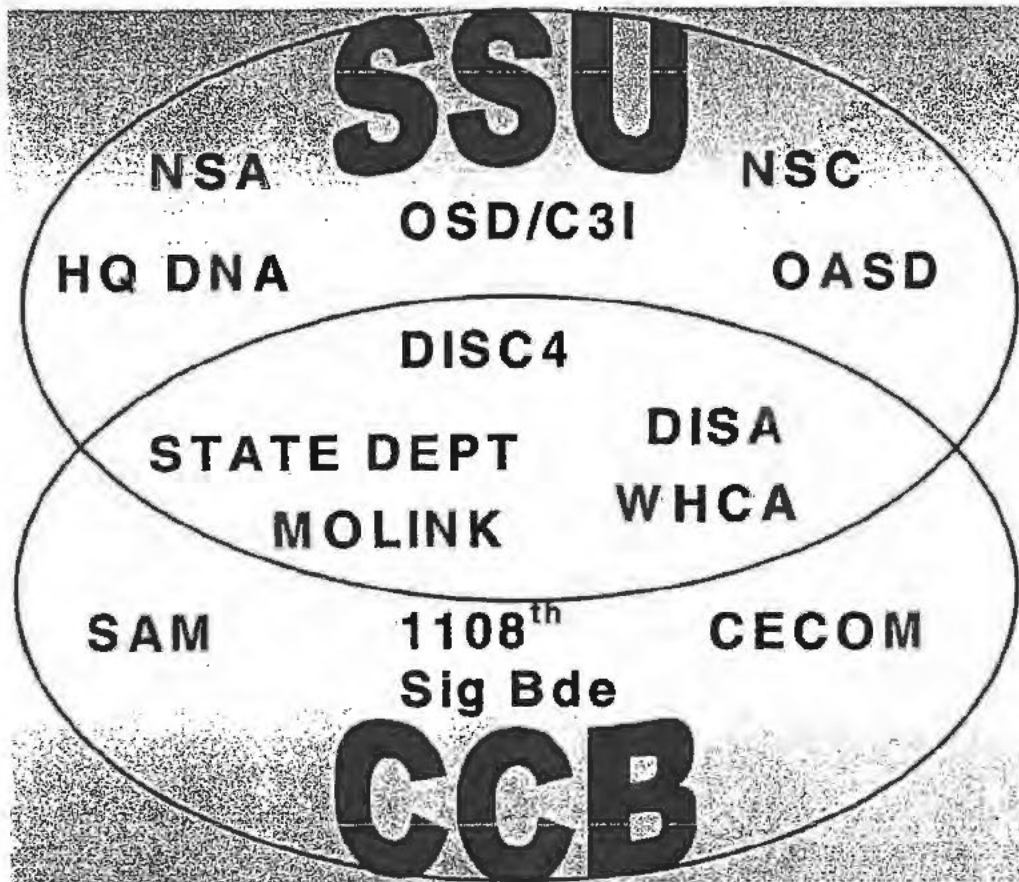


Figure 1

UNCLASSIFIED

CCB ORGANIZATION AND MEMBERSHIP

The CCB will be divided into two primary management oversight groups with responsibilities described herein.

The Configuration Control Board (CCB)

The CCB is the body within the Army that tracks the status of the DCL program and formulates courses of action to resolve problems. Direction and taskings for Army organizations come from this group. The CCB determines the level of funding required to implement DCL program decisions. The CCB then ensures the requirement is coordinated with the appropriate Army Staff (ARSTAFF) and Army Secretariat so that the necessary funding is available to execute Army budget lines that are granted for the program. The CCB Chairman will coordinate with the ARSTAFF and Army Secretariat for any funding required for the operations, maintenance, and modernization of the DCL program.

Members of the CCB are shown in Figure 2 below.

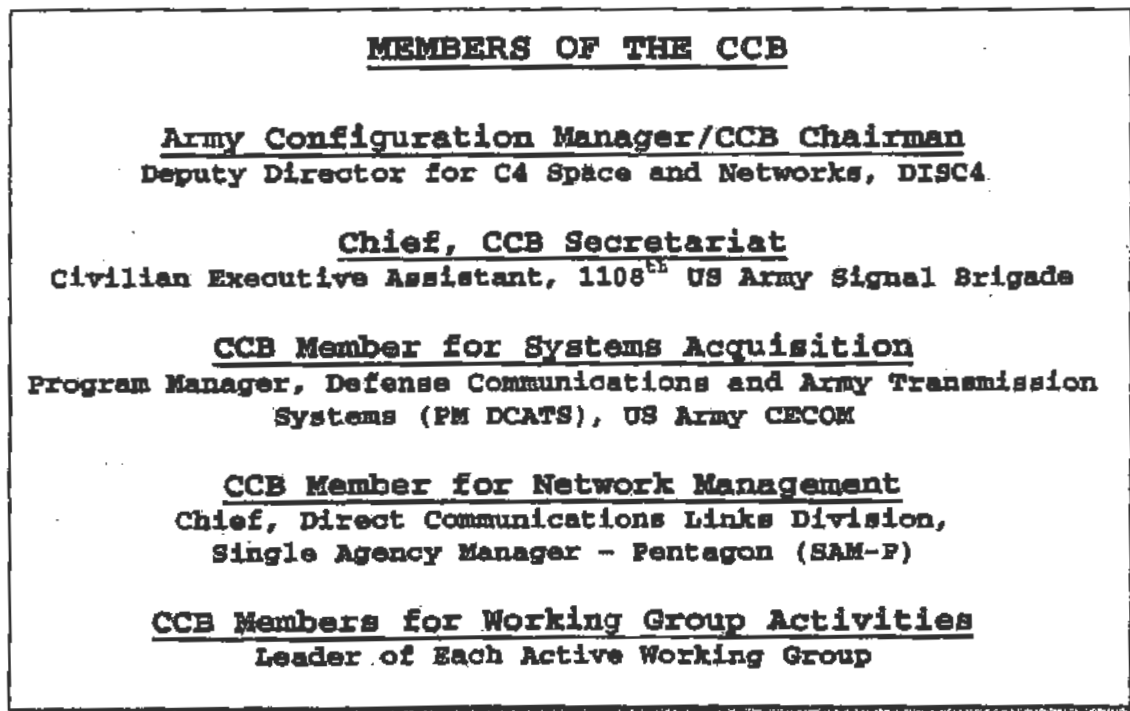


Figure 2

UNCLASSIFIED

CCB membership will consist of representation from DISC4, Single Agency Manager-Pentagon (SAM-P), 1108th US Army Signal Brigade, and Program Manager-Defense Communications and Army Transmission Systems (PM-DCATS). The DISC4 representative will hold the CCB chair position. The Civilian Executive Assistant (CEA) at the 1108th Signal Brigade will serve as Chief of the CCB Secretariat which coordinates the activities of the CCB for the Chairman, and documents actions of the CCB. Members will make decisions by casting votes, each member having one vote. Voting procedures are briefly discussed on page 9. Specific member duties and responsibilities are outlined below.

☐ **Army Configuration Manager/CCB Chairman**

The Deputy Director for the C4 Space and Networks Division (SAIS-PAC-N) within the DISC4 serves as the DCL Configuration Manager and Chairman of the Configuration Control Board. In this position, the Chairman is primarily responsible for ensuring that the Army successfully carries out its DCL Executive Agency mission for the Department of Defense (DOD). When specifically directed by the CCB Chairman to do so, the CCB Secretariat Chief will serve as CCB Chairman when the Chairman cannot attend.

☐ **Chief of the CCB Secretariat**

The Civilian Executive Assistant (CEA), 1108th U.S. Army Signal Brigade, will serve as the Chief of the CCB Secretariat. In this position, the CEA will advise the CCB of any issues that require the attention and/or decisions by the CCB. The Secretariat will advise the CCB Chairman of the need to hold meetings and will make necessary arrangements for such meetings, including the preparation of agendas and minutes. In general, the CCB Secretariat will provide the recurring administrative support required to maintain the CCB, and will participate in SSU meetings at the request of the CCB Chairman. When specifically requested, the Chief of the Secretariat will stand in for the Chairman at meetings of the CCB.

☐ **CCB Member for Systems Acquisition**

US Army Communications Electronics Command (CECOM) assists the Army in carrying out its DCL Executive Agency

NOW
21ST SIG BDE

NOW THE 21ST
SIG BDE, DEPUTY
MED

UNCLASSIFIED

mission for DOD by acquiring any new or upgraded DCL system deemed necessary by the SSU. Within CECOM, PM DCATS is designated the action agency for this specific function. PM DCATS is responsible for the overall acquisition and installation of all communications sub-systems managed by the CCB, which are approved by the SSU in response to changes in user requirements. Project funding will be managed by PM-DCATS. PM DCATS can further delegate its acquisition responsibilities to one of its subordinate Product Managers as necessary. The PM will participate in SSU meetings at the request of CCB Chairman.

☐ **CCB Member for Network Management**

The Chief of the Direct Communications Link (DCL) Division within the Office of the Single Agency Manager, Pentagon (SAM-P) will serve as the primary member on the CCB for overall network management. In this position, SAM-P advises the CCB of any issues related to the ability of the DCL circuits to maintain operational availability rates as established by bilateral agreements. Issues will include, but are not limited to, those impacting current operational performance and maintenance actions, as well as those that are needed to plan and implement future system upgrades. SAM-P will participate in SSU meetings at the request of the CCB Chairman.

☐ **CCB Members for Working Group Activities**

Working Groups will consist of two types: **Standing** and **Ad-Hoc**. Two Standing Working Groups currently exist: the Engineering and the Software Working Groups. The CCB Chairman on an as needed basis will establish other Ad-Hoc Working Groups. Ad-Hoc Working Groups will be temporary in nature to address specific DCL problems, issues, and plans. Membership and duties of the two standing working groups are described below.

The Engineering Working Group

The PM DCATS chairs the Engineering Working Group. Composition of the working group will consist primarily of engineers or technical representatives from the following organizations: (1) PM DCATS, (2) WHCA, (3) State

UNCLASSIFIED

Department, (4) DISA, (5) SAM-P, and (6) 1108th Signal Brigade. Participation of other organizations may be required as deemed necessary by PM DCATS. PM DCATS is considered the overall Army DCL System Engineer for acquisition purposes. The DISA Engineer for the Special Communications Link Program Office will provide recurring administrative support to the working group. Such support will include provision of meeting sites, preparing meeting materials including agendas, distributing meeting notices, and publishing minutes as required. In the absence of PM DCATS, the DISA Engineer will chair working group meetings. The CCB Chairman based on comments from users will assign issues for Engineering Working Group consideration. The Chief of the Engineer Working Group is a member of the CCB.

The Software Working Group

SAM-P chairs the Software Working Group. In addition to SAM-P, the following organizations will comprise the Software Working Group: (1) the National Security Agency (NSA), MOLINK, NRRC, and (as needed) the 1108th, PM DCATS, and DISA. The Software Working Group will prepare recommendations to resolve software problems and upgrade issues. Close coordination with the Engineer Working Group will be essential for effective configuration control. Recommendations will be submitted for CCB approval. The Chief of the Software Working Group is a member of the CCB.

CCB Advisory Council

The Advisory Council consists of associate CCB members who are represented at the SSU and as such have input to the requirements development and policy issues for the DCL system. Advisory Council members do not vote, but rather advise and provide guidance to the CCB on issues the CCB is considering. The primary responsibility of this group is to provide guidance and assistance to the CCB for integration of policy and directives into system architecture, technical capabilities and sustainment. The membership will consist of the following organizations: Defense Information Systems Agency (DISA) Special Communications Program Officer, the US State Department, the Joint Chiefs of Staff - Moscow Hotline (JCS-MOLINK) of the National Military Command System (NMCS), and the White House Communications Agency (WHCA). Specific duties are shown below.

UNCLASSIFIED

☐ **Defense Information System Agency (DISA)**

Director, DISA exercises program management and technical oversight of the activities pertaining to the planning, procurement, hardware/software development, installation, test, evaluation, and operational cut-over of the DCL program. DISA carries-out these activities through the National Communications System/Defense Information Systems Agency Operations Center (NCS/DISAOC). As the DOD PM for the DCL system, DISA chairs the CCB Advisory Council. In this role, DISA coordinates all activities of the CCB with organizations external to the CCB. The DISA PM will provide the CCB information on overall program concerns and agreements that apply to or have impact on the DCL program.

☐ **Department of State**

The Department of State supports the CCB and the DISA Program Manager by coordinating, as required, any configuration management or operational issues concerning the NRRC program managed by the Department of State on matters that impact any CCB/DCL managed systems. The Department of State will fund any support provided to NRRC and related systems provided by the Army in carrying out its system life cycle support responsibilities.

☐ **Joint Chiefs of Staff, Molink Branch of NMCS**

The Chief of the JCS/MOLINK Branch in the NMCS supports the CCB Advisory Council by providing input on matters concerning Joint Staff requirements for the DCL system. The Chief of the JCS/MOLINK Branch also provides operational oversight for DCL equipment upgrades.

☐ **White House Communications Agency (WHCA)**

Commander, WHCA is responsible for presidential communications and provides operational support for related direct communications systems.

UNCLASSIFIED

CCB MEMBER RESPONSIBILITIES

- ☐ Participate in the total life-cycle impact evaluation for all proposed changes. Recommending approval/disapproval or other appropriate action.
- ☐ Evaluate each change proposal relative to the immediate and future impact in their respective areas of interest, and relevant impact on other concerned organizations.
- ☐ Support any and all CCB sanctioned activities with representation. This includes taking timely action on taskings assigned by the CCB.
- ☐ Assure that all changes are in the best interest of the government.
- ☐ Present their organization's official positions relative to the disposition of each proposed change evaluated; and serve as the principal point of contact (POC) for coordinating DCL CM activities within his/her organization.
- ☐ Notify the Chairman of any change in the CCB representation from his/her organization.
- ☐ Provide necessary program funding required to participate in CCB sanctioned activities.

CCB CHAIRMAN RESPONSIBILITIES

- ☐ Notify the board members of scheduled meetings.
- ☐ Convene the board in formal session on at least a quarterly basis, or as required, for the resolution/coordination of significant issues concerning the DCL system.
- ☐ Assure the resolution of all change proposals submitted for review and action.

UNCLASSIFIED

- ☐ Represent the Army at SSU meetings in the absence the Director of Programs and Architecture in the ODISC4.
- ☐ Ensure all proposed changes are properly documented and processed for evaluation by the CCB.
- ☐ Implementing all other actions deemed necessary by the CCB to maintain an effective and coordinated CM program.

VOTING PROCEDURES

The CCB will vote on all proposals requiring an Army position or decision. This vote will be binding for all DCL sub-systems whose configuration management has been identified as an Army responsibility in the Configuration Management Plan. At least three members of the CCB present constitute a quorum. At those times when the 1108th CEA is acting as CCB Chair, the three other members of the CCB must still be present to form a quorum. No CCB member will have more than one vote regardless of the number of positions they hold. For example, a CCB member who is also leader of a working group will not have two votes even though he/she holds two positions.

CHANGES TO THE CCB CHARTER

This Charter will remain in effect for one year from the date of release unless otherwise agreed to by unanimous consent of the CCB Members. At the first anniversary of the Charter, the CCB Chairman will survey CCB to determine the adequacy of the Charter and request recommendations for proposed enhancements/modifications. Thereafter, the Charter will be reviewed every two years or unless agreed to by unanimous consent of the CCB members. Requests for changes to this charter should be submitted to the CCB Chairman for consideration.

SUBMITTING CHANGE PROPOSALS

All requests for changes to either the DCL program management documentation (DCL Charter and DCL Centralized Management Plan), or to the operational (hardware and software)

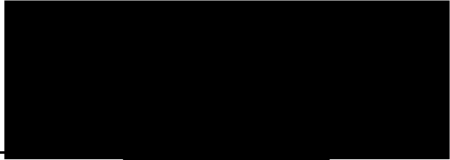
UNCLASSIFIED

capabilities of the DCL program must be fully documented. Official written proposals for either type of change must be submitted by the requesting organization according to the procedures described below.


- Proposals for changes are submitted as a Memorandum to the CCB Chairman signed by the Commander or Director of the requesting organization.
- Proposals for changes will, at a minimum, identify:
 - problems or issues that will be addressed,
 - descriptions of the proposed changes,
 - parts of the DCL program that will be involved,
 - projected benefits and impacts of the proposed changes, and
 - projected cost and schedule required to complete the enhancements.
- CCB Chairman tasks the appropriate Standing Working Group(s) to review proposals for change.
- Working Groups review proposals and submit recommended course(s) of action to the Chief of the CCB Secretariat.
- CCB Secretariat develops coordination package for all CCB and Advisory Council members.
- CCB and Advisory Council members review change proposals - CB members for voting purposes and Advisory Council members for information only.
- CCB Secretariat submits fully coordinated package for CCB consideration.
- CCB votes on proposal package that is then either signed by the CCB Chairman or returned to the CCB Secretariat for additional work.
- Signed packages are presented to the SSU for concurrence or non-concurrence.

Configuration Control Board Charter

Coordination and Approvals




Colonel, GS
Chairman,
Configuration Control Board
Department of the Army



Mr. 
Chief,
Direct Communications Link Division
Single Agency Manager – Pentagon

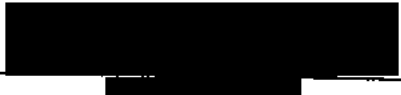

Chief,
Nuclear Risk Reduction Center
Communications,
Department of State


Program Manager,
Defense Information Systems Agency,
Special Communications Link Program
Office


Mr. 
Chief of Operations
White House Communications Agency


Mr. 
Project Manager,
Defense Communications &
Army Transmission Systems,
US Army
Communications Electronics Command


Colonel, USAF,
Chief,
Operations and Support Division,
National Military Command Center,
Office of the Joint Chiefs of Staff,
J33


Colonel, Signal Corps
Commander,
1108th US Army Signal Brigade

TAB K

TAB-D

Representatives for the following agencies/organizations constitute the voting members of the Army CWON CCB:

- Army CIO/G6 AONS Land WarNet Network Integration Division, CCB Chair, Policy
- DISA CWON Program Manager, CCB Secretary
- Army Project Manager Defense Communications and Army Transmission System (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

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 Army CWON Systems CCB:

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

5.0 Operating Procedures

- a. The Army CWON CCB will meet annually or at the call of the CCB Chair.
- b. The Army CWON 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).
- c. The CCB Chair, with support from the CCB secretary, will:
 - 1) Establish and maintain the Army CWON Systems SharePoint site that will be used to disseminate and collect CCB information and data.
 - 2) Schedule CCB meetings and locations.
 - 3) Publish meeting agendas.
 - 4) 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.
 - 5) Request CCB voting members review the advance information and formulate a vote on CCB Chair recommendations that are not anticipated to be controversial.
 - 6) Conduct CCB meetings and record meeting minutes to include an annotated list of ERs and ECPs as approved, rejected, or deferred.

TAB D

- 7) Approved ERs and ECPs will be scheduled for implementation as part of the overall Army CWON Systems schedule. Deferred ERs and ECPs will be carried over to the next CCB.
- 8) Assign action items and monitor progress to completion.
- 9) Develop and publish CCB meeting minutes to reflect the CCB discussions and decisions.
- 10) Seek voting members' consensus and decisions on urgent out-of-cycle ERs/ECPs that must be addressed before the next regularly scheduled CCB meeting.
- 11) Brief all approved ERs and ECPs to the National Leadership Command Capability (NLCC) Executive Management Board (EMB).

d. The CCB Voting members will:

- 1) Represent the interests of their organization's Army CWON Systems role by attending CCB meetings, voting and responding to advance status request and recommendations from the CCB Chair.
- 2) 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.
- 3) Complete all assigned CCB tasks in a timely manner.

e. The DISA CWON PM will:

- 1) Receive guidance for Army CWON Systems from the NLCC EMB and provide that guidance in written form to CCB voting members.
- 2) Provide CWON Program guidance in written form to the CCB voting members.
- 3) Prioritize, based on overall CWON Program Priorities and Agreements, the ERs and ECPs provided by the CCB Member, Planning, Programming and Budget.
- 4) 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.

f. The CCB Member, Planning, Programming and Budget will:

- 1) Maintain the Army CWON Systems CM Plan.
- 2) Develop and publish the process for submitting Army CWON Systems ERs and ECPs in the Army CWON Systems SharePoint or other website as decided by the CCB Chair.
- 3) Establish and maintain the Army CWON Systems ER and ECP database that contains the history of each Army CWON Systems ER and ECP submitted for CCB consideration. This will include a prioritization list of ERs and ECPs resulting from the previous Army CWON Systems CCB activities that includes whether the ER or ECP was approved, rejected or deferred and if approved, the anticipated Army CWON Systems scheduled implementation date.
- 4) Prepare ERs and ECPs for consideration by the CCB. Seek, receive, record, evaluate, categorize and prioritize Army CWON Systems ERs and ECPs from stakeholders and users. The results of these activities are:

TAB D

- a) The aggregation of similar/duplicate ERs and ECPs into single ERs and ECPs respectively and maintain an audit trail of the aggregation.
 - b) Provide aggregated ERs and ECPs to all voting CCB Members no later than six weeks prior to the next scheduled CCB meeting.
 - c) 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.
- 5) 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.
 - 6) Ensure all CCB approved ERs and ECPs are approved by the DISA CWON Program IAM prior to implementation.
 - 7) Implement, with support from the CCB Member Technical and Engineering, the ERs and ECPs in accordance with the CCB approved plan and schedule.
- g. The CCB Member, Technical and Engineering will:
- 1) Evaluate ERs and ECPs provided by the CCB Member, Planning, Programming and Budget for technical feasibility and impact to the technical capabilities of all Army CWON Systems CIs.
 - 2) Provide an estimate of the resources (in consistent units of measure) required to implement ERs and ECPs across all Army CWON Systems CIs.
 - 3) 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.
 - 4) Provide support for the implementation of the ERs and ECPs in accordance with the CCB approved plan and schedule.
- h. The CCB Member, Operations and Maintenance
- 1) 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 Army CWON Systems CIs.
 - 2) An estimate of the additional resources (in consistent units of measure) required to operate and maintain all Army CWON Systems CIs due to the ERs and ECPs.
 - 3) 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.
 - 4) Provide support for the implementation of ERs and ECPs in accordance with the CCB approved plan and schedule.

6.0 Decision-Making Process

- a. Each CCB voting member will present their evaluation of the proposed ERs and ECPs.
- b. CCB non-voting members may present additional information for each of the ERs and ECPs to the CCB.
- c. The CCB chair will call for a vote on each ER and ECP.

TAB 2

- d. An affirmative vote by the majority of voting members participating in the CCB meeting will be required to approve Army CWON Systems ERs or ECPs.
- e. 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.
- f. 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.
- g. The CCB will assign as an action item responsibility for implementation of each approved ER or ECP to the CCB Member, Planning, Programming and Budget.
- h. Other CCB voting members may be assigned action items to support the CCB Member, Planning, Programming and Budget with implementation of any approved ERs or ECPs.

7.0 Communicating Status

- a. The CCB Member, Planning, Programming and Budget will post all ER or ECP CCB decisions to the Army CWON Systems SharePoint site.
- b. The CCB Member, Planning, Programming and Budget 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.
- c. Each CCB voting member will provide advance status on ongoing ERs, ECPs, Schedule Releases, and action items to the CCB Chair bi-weekly.

8.0 Revision History

This is the original version of the Army CWON Systems CCB Charter. It is currently in Draft form.

9.0 Authorization

The DISA CWON Program Manager and the Army CWON Systems CCB Chair approve this charter.

TAB L

TAB P



DEPARTMENT OF THE ARMY
21ST SIGNAL BRIGADE
1438 PORTER STREET
FORT DETRICK MD 21702-6046

NETC-SYC

2 APR 18

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 Chief Information Officer, ATTENTION LTG Bruce Grayford, CIO-G-6, Director
(SAIS-AO), Architecture, Operations, Networks & Space (AONS), Directorate of the CIO-G-6
6, Pentagon, Washington, D.C. DC 20310

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

1. References

a. Memorandum, United States Army Network Enterprise Technology Command
Subject AR 15-6 Investigation, allegations of security risks and other improprieties present
at the Detrick Earth Station (DES), dated December 17, 2015 (Enclosure 1).

b. Memorandum, Department of the Army, 302d Signal Battalion, Subject AR 15-6
Investigation, Detrick Earth Station (DES), dated April 20, 2016 (Enclosure 2).

c. Memorandum, Department of the Army, 302d Signal Battalion, Subject AR 15-6
Investigation, Detrick Earth Station (DES) Update 1, dated January 18, 2018 (Enclosure 3).

2. Background. The Department of the Army, Office of the General Counsel (OGC),
received a referral from the United States Office of Special Counsel (OSC) to provide a
status update of outstanding actions from the Army Regulation (AR) 15-6 investigation
discussed in Enclosure 1.

a. OSC received a disclosure from a civilian army employee who alleged that the
2015 re-allocation of resources from the Detrick Earth Station (DES) to the Gateway
Telecommunications Center (GTC), located across the street from the DES, and the
accompanying reconfiguration of the DES to an unmanned satellite station under control
of the GTC, creates a substantial and specific danger to public safety. In 2015, this
whistleblower reported his concerns to Army officials who conducted an AR 15-6
investigation of the allegations (Enclosure 1). The allegations were largely
unsubstantiated, but the Army made several recommendations which the whistleblower

Formatted: Font: (Default) Arial, 11.5 pt

Formatted: Indent: First line: 0.4"

Formatted: Indent: Left: 0.4"

Formatted: Normal, Indent: First line: 0.4", No bullets or
numbering

Formatted: Font: (Default) Arial, 11.5 pt

Formatted: Font: (Default) Arial, 11.5 pt

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Indent: First line: 0.4"

Formatted: Font: (Default) Arial, 11.5 pt

Formatted: Font: (Default) Arial, 11.5 pt

Formatted: Indent: First line: 0.4"

Formatted: Font: (Default) Arial, 12 pt

NETC-SYC

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

maintains have gone unaddressed. As a result, OSC requested that Army's OSC, on behalf of the Secretary of the Army, and as the Secretary's Liaison with OSC, provide a status update as to the implementation of all of the recommendations, particularly with respect to recommendation 4a. IAW the DCL IA Plan, a chartered CCB is required to be established at the DLS.

b. In response to the OSC inquiry, Enclosure 3 provided a status update of the implementation of the recommendations addressed in Enclosure 2, including the re-establishment of the DCL Configuration Control Board (CCB).

c. Unfortunately, through administrative oversight and change in personnel at the 302d Signal Battalion, the DCL CCB was never re-established.

3. The purpose of this memorandum is to request the re-start of the Configuration Control Board (CCB) and its governance process related to the Direct Communications Link (DCL) and its subcomponents, of which the Detrick Earth Station (DES) is part of this command. Your consideration of my request will result in a final action by the Army which will be responsive to the OSC's request for a status update on the outstanding AN 15-6 recommendation.

4.2 Previously, the Direct Communications Link and its subsystems were governed by a configuration control board chaired by the AONS Directorate and of which the 21st Signal Brigade leadership served as the CCB's Secretariat. This governing body provided the necessary interactions that helped shape the systems we have today. With the pending and emerging changes in the DES configurations and its possible new mission sets, I believe it is appropriate that this CCB be re-started; or as a minimum the DCL systems be integrated into another existing governing structure.

5.3 Having a standing forum to review and collaborate on proposed and emerging changes will have benefits to the community at large and make the success of the systems more assured.

6.4. I look forward to working with you on this re-started effort.

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

COL, SC
Commanding

Enclosures

TAB M

CONFIGURATION CONTROL BOARD (CCB)

CHARTER

1.0 AUTHORITY

National Security Directive – 186 (NSD-186) provides overall guidance for continuation of the Direct Communications Link (DCL) program for the United States. This document, signed by President Ronald Reagan in November 1985, assigned Executive Agency for the National Communications System to the Secretary of Defense (SECDEF). SECDEF responsibilities under this directive include funding and implementation of the DCL program. Presidential Decision Directive/NSC-55, signed 12 March 1997 by President William Jefferson Clinton, confirmed continued maintenance of the DCL.

Deputy Under Secretary of Defense for Command, Control, Communications and Intelligence (DUSD/C3I) Memorandum, dated 14 March 1984, assigned life cycle support responsibility for the DCL program to the Department of the Army. The mission includes configuration control (hardware and software), funding, procurement, site survey, and associated engineering and installation of the U.S. portion of the DCL program. In 2000, an updated memorandum from OASD/C3I was issued that confirmed the Army's continued role as the Lead Military Department (LMD) for the DCL, responsible for life cycle management, procurement, installation, operation, training, maintenance, supply support, and Planning, Programming and Budgeting System (PPBS) responsibilities.

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. In March 1992, DUSD-C3I assigned the Army the similar support responsibilities for the Continuous Communications Link (CCL) and Government-to-Government (GGCL) programs.

The Standing Sub-Committee for Upgrades (SSU) is the SECDEF body, authorized by the President, to set technical parameters and establish overall milestone schedules for upgrading the DCL system consistent with U.S./Russian agreements and national Security Policy. The SSU assigns engineering and procurement responsibilities and tracks milestone accomplishments. According to NSD-186, the SECDEF establishes the membership of the SSU.

Army Regulation (AR) 25-1, The Army Information Resources Management Program, dated 15 July 2005, directs the CIO/G-6 to provide oversight for National Security Systems (NSS) over Army information systems and other DOD systems for which the Army has

been given responsibility, including the DCL program. This CIO/G-6 oversight is exercised through a body called the DCL Configuration Control Board (CCB). The DCL CCB is the regulatory body for controlling and evaluating software, hardware, and operational changes to the DCL system as prescribed in the Centralized Management Plan (CMP) for the DCL program.

The relationship and membership of both the SSU and CCB are depicted at Figure 1.

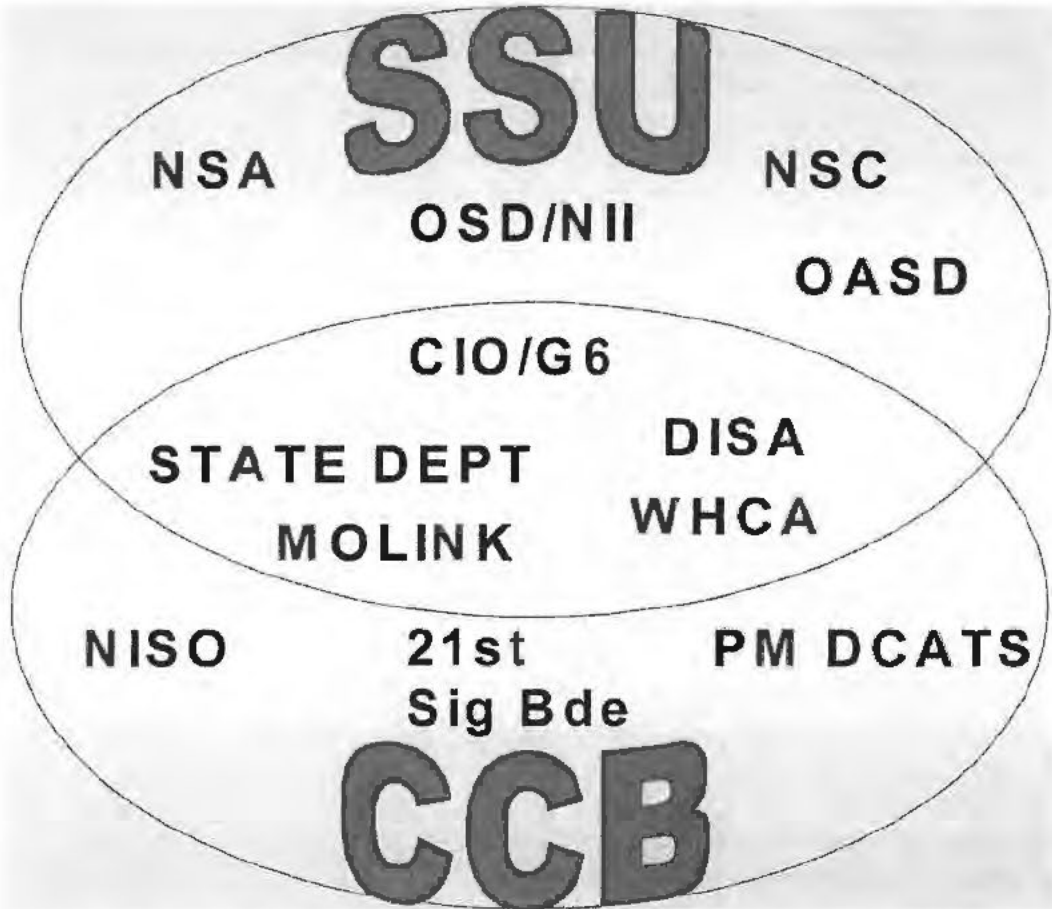


Figure 1. Relationship and Membership of the SSU and CCB.

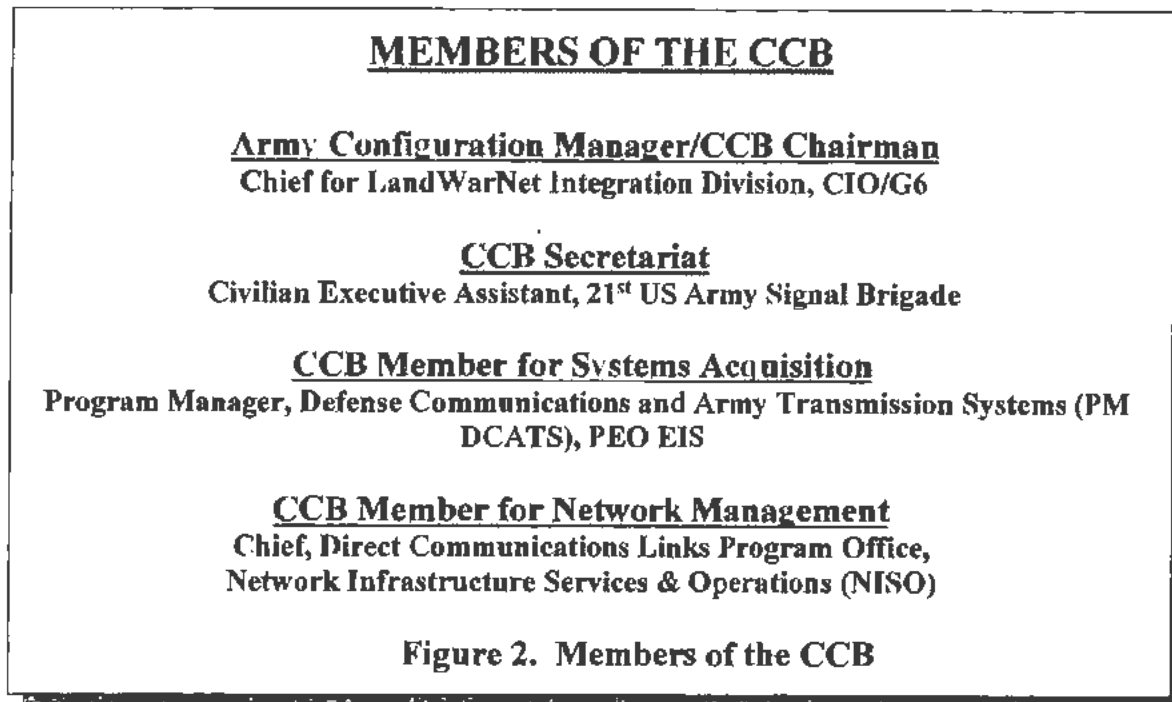
2.0 CCB ORGANIZATION AND MEMBERSHIP

The CCB will be divided into two primary management oversight groups with responsibilities described herein.

2.1 The Configuration Control Board (CCB)

The CCB is the body within the Army that tracks the status of the DCL program and formulates courses of action to resolve problems. Direction and taskings for Army organizations come from this group. The CCB determines the level of funding required to implement DCL program decisions. The CCB then ensures the requirement is coordinated with the appropriate Army Staff (ARSTAFF) and Army Secretariat so that the necessary funding is available to execute Army budget lines that are granted for the program. The CCB Chairman will coordinate with the ARSTAFF and Army Secretariat for any funding required for the operations, maintenance, and modernization of the DCL program.

Members of the CCB are shown in Figure 2 below.



CCB membership will consist of representation from CIO/G6, Network Infrastructure Services Office (NISO), 21st US Army Signal Brigade, and Program Manager-Defense Communications and Army Transmission Systems (PM-DCATS). The CIO/G6 representative will hold the CCB chair position. The Civilian Executive Assistant (CEA) at the 21st Signal Brigade will serve as Chief of the CCB Secretariat which coordinates the activities of the CCB for the Chairman, and documents actions of the CCB. Members will make decisions by casting votes, each member having one vote. Voting procedures are briefly discussed on page 9. Specific member duties and responsibilities are outlined below.

2.1.1 Army Configuration Manager/CCB Chairman

The Chief for LandWarNet Integration Division within the CIO/G6 serves as the DCL Configuration Manager and Chairman of the Configuration Control Board. In this position, the Chairman is primarily responsible for ensuring that the Army successfully carries out its DCL Lead Military Department (LMD) mission for the Department of Defense (DOD). When specifically directed by the CCB Chairman to do so, the CCB Secretariat Chief will serve as CCB Chairman when the Chairman cannot attend.

2.1.2 Chief of the CCB Secretariat

The Civilian Executive Assistant (CEA), 21st U.S. Army Signal Brigade, will serve as the Chief of the CCB Secretariat. In this position, the CEA will advise the CCB of any issues that require the attention and/or decisions by the CCB. The Secretariat will advise the CCB Chairman of the need to hold meetings and will make necessary arrangements for such meetings, including the preparation of agendas and minutes. In general, the CCB Secretariat will provide the recurring administrative support required to maintain the CCB, and will participate in SSU meetings at the request of the CCB Chairman. When specifically requested, the Chief of the Secretariat will stand in for the Chairman at meetings of the CCB.

2.1.3 CCB Member for Systems Acquisition

Program Manager Defense Communications and Army Transmission Systems (PM DCATS) within the Program Executive Office Enterprise Information Systems (PEO EIS) assists the Army in carrying out its DCL Executive Agency mission for DOD by acquiring any new or upgraded DCL system. PM DCATS is responsible for the overall acquisition and installation of all communications sub-systems managed by the CCB, which are approved by the SSU in response to changes in user requirements. Project funding for procurements associated with this program will be managed by PM-DCATS. PM DCATS can further delegate its acquisition responsibilities to one of its subordinate Product Managers as necessary. The PM will participate in SSU meetings at the request of CCB Chairman.

2.1.4 CCB Member for Network Management

The Chief of the Direct Communications Link (DCL) Division within the Network Infrastructure Services Office (NISO) will serve as the primary member on the CCB for overall network management. In this position, NISO advises the CCB of any issues related to the ability of the DCL circuits to maintain operational availability rates as established by bilateral agreements. Issues will include, but are not limited to, those impacting current operational performance and maintenance actions, as well as those that are needed to plan and implement future system upgrades. NISO will participate in SSU meetings at the request of the CCB Chairman.

2.1.5 Working Group Activities

UNCLASSIFIED

Working Groups will consist of two types: **Engineering** and **Ad-Hoc**. Membership and duties of the two standing working groups are described below.

2.1.5.1 The Engineering Working Group

The PM DCATS chairs the Engineering Working Group. Composition of the working group will consist primarily of engineers or technical representatives from the following organizations: (1) PM DCATS, (2) WHCA, (3) State Department, (4) DISA, (5) NISO, and (6) 21st Signal Brigade. Participation of other organizations may be required as deemed necessary by PM DCATS. PM DCATS is considered the overall Army DCL System Engineer for acquisition purposes. The DISA Engineer for the Special Communications Link Program Office will provide recurring administrative support to the working group. Such support will include provision of meeting sites, preparing meeting materials including agendas, distributing meeting notices, and publishing minutes as required. In the absence of PM DCATS, the DISA Engineer will chair working group meetings. The CCB Chairman based on comments from users will assign issues for Engineering Working Group consideration. The Chief of the Engineer Working Group is a member of the CCB.

2.1.5.2 Ad-Hoc Working Groups

The CCB Chairman, on an as-needed basis, can establish Ad-Hoc Working Groups. Ad-Hoc Working Groups will be temporary in nature to address specific DCL problems, issues, and plans.

2.2 CCB Advisory Council

The Advisory Council consists of associate CCB members who are represented at the SSU and as such have input to the requirements development and policy issues for the DCL system. Advisory Council members do not vote, but rather advise and provide guidance to the CCB on issues the CCB is considering. The primary responsibility of this group is to provide guidance and assistance to the CCB for integration of policy and directives into system architecture, technical capabilities and sustainment. The membership will consist of the following organizations: Defense Information Systems Agency (DISA) Senior National Leader Communications (SNLC) Program Office, the US State Department, the Joint Chiefs of Staff – Moscow Hotline (JCS-MOLINK) of the National Military Command System (NMCS), and the White House Communications Agency (WHCA). Specific duties are shown below.

2.2.1 Defense Information System Agency (DISA)

Director, DISA exercises program management and technical oversight of the activities pertaining to the planning, procurement, hardware/software development, installation, test, evaluation, and operational cut-over of the DCL program. As the DOD PM for the DCL system,

UNCLASSIFIED

DISA chairs the CCB Advisory Council. In this role, DISA coordinates all activities of the CCB with organizations external to the CCB. The DISA PM will provide the CCB information on overall program concerns and agreements that apply to or have impact on the DCL program.

2.2.2 Department of State

The Department of State supports the CCB and the DISA Program Manager by coordinating, as required, any configuration management or operational issues concerning the NRRC program managed by the Department of State on matters that impact any CCB/DCL managed systems. The Department of State will fund any support provided to NRRC and related systems provided by the Army in carrying out its system life cycle support responsibilities.

2.2.3 Joint Chiefs of Staff, Molink Branch of NMCS

The Chief of the JCS/MOLINK Branch in the NMCS supports the CCB Advisory Council by providing input on matters concerning Joint Staff requirements for the DCL system. The Chief of the JCS/MOLINK Branch also provides operational oversight for DCL equipment upgrades.

2.2.4 White House Communications Agency (WHCA)

Commander, WHCA is responsible for presidential communications and provides operational support for related direct communications systems.

3.0 CCB MEMBER RESPONSIBILITIES

- Participate in the total life-cycle impact evaluation for all proposed changes. Recommending approval/disapproval or other appropriate action.
- Evaluate each change proposal relative to the immediate and future impact in their respective areas of interest, and relevant impact on other concerned organizations.
- Support any and all CCB sanctioned activities with representation. This includes taking timely action on taskings assigned by the CCB.
- Assure that all changes are in the best interest of the government.
- Present their organization's official positions relative to the disposition of each proposed change evaluated; and serve as the principal point of contact (POC) for coordinating DCL CM activities within his/her organization.
- Notify the Chairman of any change in the CCB representation from his/her organization.
- Provide necessary program funding required to participate in CCB sanctioned activities.

4.0 CCB CHAIRMAN RESPONSIBILITIES

- Notify the board members of scheduled meetings.
- Convene the board in formal session on at least a quarterly basis, or as required, for the resolution/coordination of significant issues concerning the DCL system.
- Assure the resolution of all change proposals submitted for review and action.
- Represent the Army at SSU meetings in the absence the Director of Architectures, Operations, Networks, and Space in the CIO/G6.
- Ensure all proposed changes are properly documented and processed for evaluation by the CCB.
- Implement all other actions deemed necessary by the CCB to maintain an effective and coordinated CM program.

5.0 VOTING PROCEDURES

The CCB will vote on all proposals requiring an Army position or decision. This vote will be binding for all DCL sub-systems whose configuration management has been identified as an Army responsibility in the Centralized Management Plan. At least three members of the CCB present constitute a quorum. At those times when the 21st CEA is acting as CCB Chair, the three other members of the CCB must still be present to form a quorum. No CCB member will have more than one vote regardless of the number of positions they hold.

The US and Russian Federation governments are equal partners in maintaining and operating the DCL. In order to be responsive to the needs of the bilateral decision-making process, CCB coordination and voting on change proposals may take place through direct correspondence and email discussion vice a CCB when required.

6.0 CHANGES TO THE CCB CHARTER

This Charter will remain in effect for one year from the date of release unless otherwise agreed to by unanimous consent of the CCB Members. At the first anniversary of the Charter, the CCB Chairman will survey CCB to determine the adequacy of the Charter and request recommendations for proposed enhancements/modifications. Thereafter, the Charter will be reviewed every two years or unless agreed to by unanimous consent of the CCB members. Requests for changes to this charter should be submitted to the CCB Chairman for consideration.

7.0 SUBMITTING CHANGE PROPOSALS

All requests for changes to either the DCL program management documentation or to the operational (hardware and software) capabilities of the DCL program must be fully documented.

UNCLASSIFIED

Official written proposals for either type of change must be submitted by the requesting organization according to the procedures described below.

- Proposals for changes are submitted as a Memorandum to the CCB Chairman signed by the Commander or Director of the requesting organization.
- Proposals for changes will, at a minimum, identify:
 - problems or issues that will be addressed,
 - descriptions of the proposed changes,
 - parts of the DCL program that will be involved,
 - projected benefits and impacts of the proposed changes, and
 - projected cost and schedule required to complete the enhancements.
- CCB Chairman tasks the appropriate Standing Working Group(s) to review proposals for change.
- Working Groups review proposals and submit recommended course(s) of action to the Chief of the CCB Secretariat.
- CCB Secretariat develops coordination package for all CCB and Advisory Council members.
- CCB and Advisory Council members review change proposals – CB members for voting purposes and Advisory Council members for information only.
- CCB Secretariat submits fully coordinated package for CCB consideration.
- CCB votes on proposal package that is then either signed by the CCB Chairman or returned to the CCB Secretariat for additional work.
- Signed packages are presented to the SSU for concurrence or non-concurrence.

TAB N

DRAFT
Regional Hub Node
System Identification Profile

TAB R

7-Mar-08

1	System ID:	
2	System Component: Governing DoD Component IA	Satellite antenna and antenna electronics.
3	Program:	USA NEICOM/9TH SC
4	System name:	Direct Communications Link (DCL) Satellite Communications (SATCOM) Terminal
5	System Acronym: System Version or Release	DST
6	Number:	???
7	System Description:	The Fort Detrick Direct Communications Link (DCL) Satellite Communications (SATCOM) Terminal is a dedicated satellite link station for special heads of state communications. The DCL SATCOM terminal is a Radio Frequency (RF) satellite communications (C - band) terminal used to take the Intermediate Frequency (IF) signal from baseband equipment, upconvert it to RF (5.85-6.65 GHz frequency range), and amplify it for the antenna's uplink transmission to a satellite. On the receive side the DCL terminal receives the RF signal from the satellite downconverts it to an IF and sends it back to baseband equipment at the Fort Detrick site.
8	DIACAP Activity:	Concurrence to list DCL as accreditation not required on the Army Portfolio Management Solution (APMS)
9	System Life Cycle or Acquisition Phase:	MS-C
10	Information System Type:	Fixed SATCOM facility
11	MAC:	MAC II
12	Confidentiality Level:	Sensitive
13	Mission Criticality :	ME
14	Accreditation Vehicle:	DODI 8500.2 and BBP for SATCOM terminals
15	Additional Accreditation Vehicles:	None
16	Certification Date:	TBD

DRAFT

DIACAP Team Roles, Member

17 Names and Contact Information	See Table Below.
18 Accreditation Status:	None
19 Accreditation Date:	Accreditation date not required
20 Authorization Termination Date:	Authorization termination date not required
21 Acquisition Category (ACA):	N/A
22 Type of IT Investment:	Infrastructure
23 Software Category:	COTS
24 Privacy Impact Assessment:	N/A
E-Authentication Risk	
25 Assessment:	N/A
26 Annual Security Review Date:	N/A
27 System Operation:	Army owned and Operated
28 Contingency Plan:	Yes
29 Contingency Plan Tested:	Yes

DIACAP Team Roles, Member Names and Contact Information

	Name	Phone	Email
PM/SM:	[REDACTED]	(732) 532-3281	[REDACTED]@us.army.mil
IAM:	[REDACTED]	732 532 2373	[REDACTED]@us.army.mil
User Representative:	[REDACTED]	(301) 619-7411, (301) 619-3518	[REDACTED]@us.army.mil, [REDACTED]s.army.mil
DAA:	[REDACTED]	(703) 806-4235	[REDACTED]@us.army.mil
IAPM:	[REDACTED]	(703) 806-2143	[REDACTED]@us.army.mil
CA:	[REDACTED]	(703) 602-7403	[REDACTED]@us.army.mil
CAR:	[REDACTED]	(703) 602-7369	[REDACTED]@us.army.mil
ACA:	[REDACTED]	732-532-4128	[REDACTED]@us.army.mil
IASO:	[REDACTED]	732-532-2373	[REDACTED]@us.army.mil
Cert. Team Lead:	[REDACTED]	732-532-2373	[REDACTED]@us.army.mil
SME:	[REDACTED]	732 532 2578, 732 532 5509	[REDACTED]us.army.mi [REDACTED]s.army.mil

TAB O



Department of Defense INSTRUCTION

TAB S

NUMBER 8500.01

March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference (d)), DoDI 8552.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (k)), and Directive-type Memorandum (DTM) 08-060 (Reference (l)).

c. Establishes the positions of DoD principal authorizing official (PAO) (formerly known as principal accrediting authority) and the DoD Senior Information Security Officer (SISO) (formerly known as the Senior Information Assurance Officer) and continues the DoD Information Security Risk Management Committee (DoD ISRMC) (formerly known as the Defense Information Systems Network (DISN)/Global Information Grid (GIG) Flag Panel).

d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term "information assurance (IA)."

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 DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

(2) All DoD IT.

(3) All DoD information in electronic format.

(4) Special access program (SAP) information technology, other than SAP ISs handling sensitive compartmented information (SCI) material.

b. Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of SCI as directed by Executive Order 12333 (Reference (n)) and other laws and regulations.

3. POLICY. It is DoD policy that:

a. Risk Management

(1) DoD will implement a multi-tiered cybersecurity risk management process to protect U.S. interests, DoD operational capabilities, and DoD individuals, organizations, and assets from the DoD Information Enterprise level, through the DoD Component level, down to the IS level as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 (Reference (o)) and Committee on National Security Systems (CNSS) Policy (CNSSP) 22 (Reference (p)).

(2) Risks associated with vulnerabilities inherent in IT, global sourcing and distribution, and adversary threats to DoD use of cyberspace must be considered in DoD employment of capabilities to achieve objectives in military, intelligence, and business operations.

(3) All DoD IT will be assigned to, and governed by, a DoD Component cybersecurity program that manages risk commensurate with the importance of supported missions and the value of potentially affected information or assets.

(4) Risk management will be addressed as early as possible in the acquisition of IT and in an integrated manner across the IT life cycle.

(5) Documentation regarding the security posture of DoD IS and PIT systems will be made available to promote reciprocity as described in DoDI 8510.01 (Reference (q)) and to assist authorizing officials (AOs) (formerly known as designated approving or accrediting authorities) from other organizations in making credible, risk-based decisions regarding the acceptance and use of systems and the information that they process, store, or transmit.

b. Operational Resilience. DoD IT will be planned, developed, tested, implemented, evaluated, and operated to ensure that:

(1) Information and services are available to authorized users whenever and wherever required according to mission needs, priorities, and changing roles and responsibilities.

(2) Security posture, from individual device or software object to aggregated systems of systems, is sensed, correlated, and made visible to mission owners, network operators, and to the DoD Information Enterprise consistent with DoDD 8000.01 (Reference (r)).

(3) Whenever possible, technology components (e.g., hardware and software) have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention. Attempts made to reconfigure, self-defend, and recover should produce an incident audit trail.

c. Integration and Interoperability

(1) Cybersecurity must be fully integrated into system life cycles and will be a visible element of organizational, joint, and DoD Component IT portfolios.

(2) Interoperability will be achieved through adherence to DoD architecture principles, adopting a standards-based approach, and by all DoD Components sharing the level of risk necessary to achieve mission success.

(3) All interconnections of DoD IT will be managed to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.

d. Cyberspace Defense. Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DoD information networks. Cyberspace defense information will be shared with all appropriately cleared and authorized personnel in support of DoD enterprise-wide situational awareness.

e. Performance

(1) Implementation of cybersecurity will be overseen and governed through the integrated decision structures and processes described in this instruction.

(2) Performance will be measured, assessed for effectiveness, and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with Sections 11103 and 11313 of Title 40, United States Code (U.S.C.) (Reference (s)).

(3) Data will be collected to support reporting and cybersecurity management activities across the system life cycle.

(4) Standardized IT tools, methods, and processes will be used to the greatest extent possible to eliminate duplicate costs and to focus resources on creating technologically mature and verified solutions.

f. DoD Information. All DoD information in electronic format will be given an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection.

g. Identity Assurance

(1) Identity assurance must be used to ensure strong identification, authentication, and eliminate anonymity in DoD IS and PIT systems.

(2) DoD will public key-enable DoD ISs and implement a DoD-wide Public Key Infrastructure (PKI) solution that will be managed by the DoD PKI Program Management Office in accordance with DoDI 8520.02 (Reference (t)).

(3) Biometrics used in support of identity assurance will be managed in accordance with DoDD 8521.01 (Reference (u)).

h. Information Technology

(1) All IT that receives, processes, stores, displays, or transmits DoD information will be acquired, configured, operated, maintained, and disposed of consistent with applicable DoD cybersecurity policies, standards, and architectures.

(2) Risks associated with global sourcing and distribution, weaknesses or flaws inherent in the IT, and vulnerabilities introduced through faulty design, configuration, or use will be managed, mitigated, and monitored as appropriate.

(3) Cybersecurity requirements must be identified and included throughout the lifecycle of systems including acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DoD IT supporting DoD tasks and missions.

i. Cybersecurity Workforce

(1) Cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with this instruction and DoD 5200.2-R (Reference (v)), and qualified in accordance with DoDD 8570.01 (Reference (w)) and supporting issuances.

(2) Qualified cybersecurity personnel must be identified and integrated into all phases of the system development life cycle.

j. Mission Partners

(1) Capabilities built to support cybersecurity objectives that are shared with mission partners will be consistent with guidance contained in Reference (r) and governed through integrated decision structures and processes described in this instruction.

(2) DoD-originated and DoD-provided information residing on mission partner ISs must be properly and adequately safeguarded, with documented agreements indicating required levels of protection.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. INFORMATION COLLECTION REQUIREMENTS. The DoD Federal Information Security Management Act (FISMA) Annual Report with Quarterly Updates, referred to in paragraphs 1v and 13q of Enclosure 2 and paragraph 12i of Enclosure 3 of this instruction, has been assigned report control symbol DD-CIO(A,Q)2296 in accordance with the procedures in DTM 12-004 (Reference (x)) and DoD 8910.1-M (Reference (y)).

7. RELEASABILITY. Unlimited. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This instruction:

- a. Is effective March 14, 2014.
- b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoDI 5025.01 (Reference (z)).
- c. Will expire effective March 14, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (z).



Teresa M. Takai
DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....	8
ENCLOSURE 2: RESPONSIBILITIES.....	14
DoD CIO.....	14
DIRECTOR, DISA	16
USD(AT&L)	17
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR DT&E (DASD(DT&E))	18
DOT&E.....	19
USD(P).....	19
USD(P&R).....	19
USD(I).....	19
DIRNSA/CHCSS.....	20
DIRECTOR, DEFENSE SECURITY SERVICE (DSS).....	21
DIRECTOR, DIA	21
DEPUTY CHIEF MANAGEMENT OFFICER (DCMO)	22
OSD AND DoD COMPONENT HEADS.....	22
CJCS	25
COMMANDER, USSTRATCOM	25
ENCLOSURE 3: PROCEDURES.....	27
INTRODUCTION	27
RISK MANAGEMENT.....	27
OPERATIONAL RESILIENCE.....	31
INTEGRATION AND INTEROPERABILITY.....	32
CYBERSPACE DEFENSE	33
PERFORMANCE.....	34
DoD INFORMATION.....	35
IDENTITY ASSURANCE.....	36
INFORMATION TECHNOLOGY	37
CYBERSECURITY WORKFORCE.....	44
MISSION PARTNERS.....	44
DoD SISO	46
DoD COMPONENT CIOs	47
DoD RISK EXECUTIVE FUNCTION.....	48
PAO.....	48
AO.....	48
ISOs OF DoD IT.....	49
ISSM	49
ISSO.....	50
PRIVILEGED USERS (E.G. SYSTEM ADMINISTRATOR).....	51
AUTHORIZED USERS	51

GLOSSARY52

 PART I. ABBREVIATIONS AND ACRONYMS52

 PART II. DEFINITIONS.....55

FIGURE

 1. Three-Tiered Approach to Risk Management28

 2. DoD Information Technology.....38

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 8500.01, "Information Assurance (IA)," October 4, 2002 (hereby cancelled)
- (b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013
- (c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003 (hereby cancelled)
- (d) DoD Directive C-5200.19, "Control of Compromising Emanations (U)," May 16, 1995 (hereby cancelled)
- (e) DoD Instruction 8552.01, "Use of Mobile Code Technologies in DoD Information Systems," October 23, 2006 (hereby cancelled)
- (f) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001 (hereby cancelled)
- (g) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Certification and Accreditation Requirements for DoD-wide Managed Enterprise Services Procurements," June 22, 2006 (hereby cancelled)
- (h) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Use of Peer-to-Peer (P2P) File-Sharing Applications Across DoD," November 23, 2004 (hereby cancelled)
- (i) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006 (hereby cancelled)
- (j) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Encryption of Sensitive Unclassified Data At Rest on Mobile Computing Devices and Removable Storage Media," July 3, 2007 (hereby cancelled)
- (k) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Protection of Sensitive Department of Defense (DoD) Data at Rest On Portable Computing Devices," April 18, 2006 (hereby cancelled)
- (l) Directive-type Memorandum 08-060, "Policy on Use of Department of Defense (DoD) Information Systems — Standard Consent Banner and User Agreement," May 9, 2008, as amended (hereby cancelled)
- (m) National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cybersecurity Policy," January 8, 2008¹
- (n) Executive Order 12333, "United States Intelligence Activities," as amended
- (o) National Institute of Standards and Technology Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," current edition
- (p) Committee on National Security Systems Policy 22, "Policy on Information Assurance Risk Management for National Security Systems," January 2012, as amended

¹ Document is classified TOP SECRET. To obtain a copy, fax a request to the Homeland Security Council Executive Secretary at 202-456-5158 and the National Security Council's Senior Director for Records and Access Management at 202-456-9200.

- (q) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
- (r) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
- (s) Title 40, United States Code
- (t) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
- (u) DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008
- (v) DoD 5200.2-R, "Personnel Security Program," January 1, 1987, as amended
- (w) DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004
- (x) Directive-type Memorandum 12-004, "DoD Internal Information Collections," April 24, 2012, as amended
- (y) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (z) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended
- (aa) Title 44, United States Code
- (ab) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (ac) DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005
- (ad) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
- (ae) DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, as amended
- (af) Deputy Secretary of Defense Memorandum, "Delegation of Authority to Negotiate and Conclude International Agreements on Cooperation in Information Assurance and Computer Network Defense," March 5, 2002²
- (ag) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
- (ah) Joint DoD/Intelligence Community memorandum, "Establishment of a Department of Defense (DoD)/Intelligence Community (IC) Unified Cross Domain Management Office (UCDMO)," July 15, 2006
- (ai) Unified Cross Domain Management Office Charter, March 21, 2007
- (aj) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum/Commander, U.S. Strategic Command Memorandum, "Establishment of the Department of Defense Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group," September 11, 2003
- (ak) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
- (al) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," as amended
- (am) Chairman of the Joint Chiefs of Staff Instruction 6211.02, "Defense Information System Network (DISN) Responsibilities," current edition
- (an) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004

² Requests for copies can be forwarded to the DoD CIO.

- (ao) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010
- (ap) Charter Defense Information Systems Network Security Accreditation Working Group, March 26, 2004²
- (aq) Defense Information System Network Global Information Grid Flag Panel Charter, April 2012, as amended²
- (ar) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
- (as) DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013
- (at) DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004
- (au) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- (av) Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013
- (aw) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004
- (ax) Section 1043 of Public Law 106-65, "Information Assurance Initiative," October 5, 1999
- (ay) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense," July 16, 2008, as amended
- (az) DoD Instruction 5134.16, "Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))," August 19, 2011
- (ba) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
- (bb) DoD Instruction 5134.17, "Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E))," October 25, 2011
- (bc) Director, Operational Test and Evaluation Memorandum, "Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs," January 21, 2009³
- (bd) Director, Operational Test and Evaluation Memorandum, "Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs," November 4, 2010⁴
- (be) Director, Operational Test and Evaluation Memorandum, "Test and Evaluation of Information Assurance in Acquisition Programs," February 1, 2013
- (bf) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010
- (bg) Committee on National Security Systems Policy 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products," June 2013, as amended
- (bh) Title 10, United States Code
- (bi) Committee on National Security Systems Policy 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," October 1, 2012
- (bj) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

³ Available at http://www.dote.osd.mil/pub/policies/2009/20090121Procedure_forOTEofIAinAcqPrograms.pdf.

⁴ Available at http://www.dote.osd.mil/pub/policies/2010/20101104Clarification_ofProcedures_forOTE_ofIA_inAcqProgs.pdf.

- (bk) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
- (bl) DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001
- (bm) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012
- (bn) DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing," October 9, 2007
- (bo) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
- (bp) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
- (bq) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (br) Committee on National Security Systems Instruction 1010, "24 x 7 Computer Incident Response Capability (CIRC) on National Security Systems," October 3, 2012
- (bs) DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
- (bt) DoD Instruction 1400.25, Volume 731, "DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees," August 24, 2012
- (bu) Title 29, United States Code
- (bv) National Institute of Standards and Technology Special Publication 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," current edition
- (bw) DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended
- (bx) DoD Chief Information Officer Memorandum, "Cross Domain Support Element (CDSE) Responsibilities," October 11, 2011
- (by) DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012, as amended
- (bz) DoD 5220.22-R, "Industrial Security Regulation," April 12, 1985
- (ca) Committee on National Security Systems Policy 300, "National Policy on Control of Compromising Emanations," April 2004, as amended
- (cb) Committee on National Security Systems Instruction 7000, "TEMPEST Countermeasures for Facilities," May 2004, as amended
- (cc) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (cd) Unified Command Plan, current edition
- (ce) Chairman of the Joint Chiefs of Staff Instruction 6510.01, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
- (cf) National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," current edition
- (cg) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
- (ch) National Institute of Standards and Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," current edition
- (ci) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended

- (cj) National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," current edition
- (ck) National Institute of Standards and Technology Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems," current edition
- (cl) Section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, January 7, 2011
- (cm) DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009
- (cn) Secretary of Defense Memorandum, "Maintaining Readiness to Operate in Cyberspace Domain," December 7, 2012
- (co) DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
- (cp) National Institute of Standards and Technology Special Publication 800-126, "The Technical Specification for Security Content Automation Protocol (SCAP): SCAP Version 1.0," current edition
- (cq) DoD O-8530.01-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," December 17, 2003
- (cr) DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008
- (cs) National Institute of Standards and Technology Special Publication 800-137, "Information Security Continuous Monitoring," current edition
- (ct) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011
- (cu) DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010
- (cv) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended
- (cw) Chairman of the Joint Chiefs of Staff Instruction 3170.01, "Joint Capabilities Integration and Development System," January 10, 2012
- (cx) DoD Directive 7045.14, "The Planning, Programming, Budgeting, and Execution (PPBE) Process," January 25, 2013
- (cy) DoD Chief Information Officer Memorandum, "Department of Defense Chief Information Officer Executive Board Charter," July 7, 2005
- (cz) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
- (da) DoD Instruction 8320.02, "Sharing Data Information, and Technology (IT) Services in the Department of Defense," August 5, 2013
- (db) DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006
- (dc) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
- (dd) DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012
- (de) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- (df) DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
- (dg) DoD Manual 5205.02, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008

- (dh) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
- (di) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Document Streamlining Program Protection Plan," July 18, 2011
- (dj) Section 811 of Public Law 106-398, "National Defense Authorization Fiscal Year 2001," October 30, 2000
- (dk) DoD Instruction 8581.01, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 8, 2010
- (dl) Committee on National Security Systems Instruction 4004.1, "Destruction and Emergency Protection Procedures for COMSEC and Classified Material," August 2006, as amended
- (dm) National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," current edition
- (dn) DoD Architecture Framework Version 2.02, August 2010⁵
- (do) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," May 19, 2011
- (dp) DoD Instruction 2030.08, "Implementation of Trade Security Controls (TSC) for Transfers of DoD U.S. Munitions List (USML) and Commerce Control List (CCL) Personal Property to Parties Outside DoD Control," May 23, 2006
- (dq) DoD Instruction 1035.01, "Telework Policy," April 4, 2012
- (dr) National Institute of Standards and Technology Special Publication 800-114, "Users Guide to Securing External Devices for Telework and Remote Access," current edition
- (ds) National Institute of Standards and Technology Special Publication 800-147, "Basic Input/Output System (BIOS) Protection Guidelines," current edition
- (dt) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Coalition Public Key Infrastructure, X.509 Certificate Policy," current edition
- (du) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (dv) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
- (dw) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008
- (dx) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
- (dy) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
- (dz) Committee on National Security Systems Instruction Number 4009, "National Information Assurance (IA) Glossary," April 26, 2010, as amended
- (ea) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," current edition
- (eb) National Institute of Standards and Technology Special Publication 800-63, "Electronic Authentication Guideline," current edition

⁵ Available at <http://dodcio.defense.gov/dodaf20.aspx>.

ENCLOSURE 2
RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Monitors, evaluates, and provides advice to the Secretary of Defense regarding all DoD cybersecurity activities and oversees implementation of this instruction.

b. Develops and establishes DoD cybersecurity policy and guidance consistent with this instruction and in accordance with applicable federal law and regulations.

c. Appoints a DoD SISO in accordance with section 3541 of Title 44, U.S.C. (Reference (aa)).

d. Coordinates with the Under Secretary of Defense for Policy (USD(P)) to ensure that cybersecurity strategies and policies are aligned with overarching DoD cyberspace policy and, in accordance with DoDD 5230.11 (Reference (ab)), support policies relating to the disclosure of classified military information to foreign governments and international organizations.

e. Coordinates with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) to:

(1) Ensure personnel identity policies and cybersecurity policies and capabilities are aligned and mutually supportive.

(2) Develop cybersecurity workforce management policies and capabilities to support identification and qualifications for a professional cybersecurity workforce.

f. Coordinates with the Under Secretary of Defense for Intelligence (USD(I)) to ensure that cybersecurity policies and capabilities are aligned with and mutually supportive of personnel, physical, industrial, information, and operations security policies and capabilities.

g. Coordinates with NIST in development of cybersecurity-related standards and guidelines.

h. Maintains a formal coordination process with the Intelligence Community (IC) Chief Information Officer (CIO) to ensure proper protection of IC information within DoD, reciprocity of IS authorization and cybersecurity risk management processes, and alignment of cybersecurity.

i. Coordinates with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) to ensure that cybersecurity responsibilities are integrated into processes for DoD acquisition programs, including research and development.

j. Coordinates with the Director, Operational Test and Evaluation (DOT&E) to ensure that cybersecurity responsibilities are integrated into the operational testing and evaluation for DoD acquisition programs.

k. Coordinates and advocates resources for DoD-wide cybersecurity solutions, including overseeing appropriations allocated to the DoD cybersecurity program.

l. Appoints a PAO for DoD ISs and PIT systems governed by the Enterprise Information Environment Mission Area (MA) (EIEMA) as described in DoDD 8115.01 (Reference (ac)).

m. Coordinates with the DoD MA owners to ensure that cybersecurity responsibilities are addressed for all DoD IT.

n. Coordinates with the USD(P) and USD(I) on integrating Defense Industrial Base (DIB) cybersecurity threat information-sharing activities and enhancing DoD and DIB cyber situational awareness in accordance with DoDI 5205.13 (Reference (ad)) and in support of DoDD 3020.40 (Reference (ae)).

o. Develops policy for negotiating, performing, and concluding agreements with international partners to engage in cooperative international cybersecurity activities, in coordination with the USD(P), USD(I), and the Director, National Security Agency (NSA)/Chief, Central Security Service (DIRNSA/CHCSS).

p. Negotiates and concludes agreements with international partners to engage in cooperative international cybersecurity and cyberspace defense activities, according to authority described in Deputy Secretary of Defense Memorandum (Reference (af)) and subject to the provisions of DoDD 5530.3 (Reference (ag)), in coordination with the:

(1) USD(P).

(2) General Counsel of the Department of Defense.

(3) Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense.

(4) USD(I), when such agreements materially affect cleared industry.

(5) CJCS.

q. Establishes policy for the life cycle management of cross-domain (CD) solutions (CDSs). This policy will address shared risk, in coordination with the IC CIO and with the direct support from the DoD/IC Unified Cross Domain Management Office (UCDMO) in accordance with Joint DoD/IC Memorandum (Reference (ah)) and the UCDMO Charter (Reference (ai)).

r. Develops and implements policy regarding continuous monitoring of DoD IT with direct support from NSA/CSS and Defense Information Systems Agency (DISA), and input from the other DoD Components.

s. Appoints a military officer in the grade of O-6 or an equivalent civilian employee as the Defense IA Security Accreditation Working Group (DSAWG) Chair.

t. Develops and implements policy for cybersecurity workforce awareness, education, training, and qualification in coordination with the USD(P&R).

u. Maintains a Defense-wide view of cybersecurity resources that supports national, organizational, joint, and DoD Component cybersecurity program planning.

v. Conducts an annual assessment of DoD Component cybersecurity programs as required by section 3545 of Reference (aa).

w. Co-chairs the Enterprise-wide IA and Computer Network Defense Solutions Steering Group (ESSG) in accordance with the ASD(NII)/DoD CIO/Commander, U.S. Strategic Command Memorandum (Reference (aj)).

x. Ensures that compromising emanations (i.e., TEMPEST) countermeasures implemented within DoD comply with current national policies.

y. Ensures compliance with the requirements of National Security Directive 42 (Reference (ak)) and collaborate with the DIRNSA/CHCSS on the performance of DIRNSA/CHCSS duties, pursuant to Reference (ak), as the National Manager for National Security Telecommunications and Information Systems Security.

2. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 13 of this enclosure, the Director, DISA:

a. Develops, implements, and, in coordination with Commander, U.S. Strategic Command (USSTRATCOM), manages cybersecurity for the DISN, consistent with this instruction and its supporting guidance.

b. Develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible.

c. Develops or acquires solutions that support cybersecurity objectives for use throughout DoD via the ESSG process in accordance with Reference (aj).

d. Establishes and maintains the IA Support Environment (IASE) in accordance with

Office of Management and Budget Circular A-130 (Reference (al)) as the DoD knowledge repository for cybersecurity related policy, guidance, and information.

e. Oversees and maintains the connection approval process in accordance with CJCS Instruction (CJCSI) 6211.02 (Reference (am)), CD connection policy as issued by DoD CIO, DoDI 8551.01 (Reference (an)), and DoDI 8100.04 (Reference (ao)) for the DISN (e.g., the Secret Internet Protocol Router Network (SIPRNet) and the Non-Classified Internet Protocol Router Network (NIPRNet)) in coordination with the DSAWG (Reference (ap)) and DoD ISRMC (Reference (aq)), when appropriate.

f. Facilitates multinational information sharing efforts, as well as information sharing between the DoD Components and eligible foreign nations in support of approved international cybersecurity and cyberspace defense agreements.

g. Supports training, exercises, workforce development, network evaluation, and other efforts to build international partner cybersecurity and cyberspace defense capacity.

h. Provides enterprise CD services compliant with the UCDMO-managed CDS Baseline List of validated solutions posted on the SIPRNet and the Joint Worldwide Intelligence Communications System (JWICS) UCDMO Intelink sites. Working with UCDMO, integrates new CD requirements into DoD Enterprise CD services.

i. Ensures the continued development and maintenance of guidance and standards procedures to catalog, regulate, and control the use and management of Internet protocols, data services, and associated ports on DoD networks, in accordance with Reference (an).

j. Develops and provides cybersecurity training and awareness products and a distributive training capability to support the DoD Components in accordance with Reference (w) and post the training materials on the IASE Website (<http://iase.disa.mil/>).

k. Conducts command cyber readiness inspections and operational risk assessments in support of USSTRATCOM.

l. Coordinates with the USD(I) to ensure command cyber readiness inspection guidance and metrics provide a unity of effort among the security disciplines (i.e., personnel, physical, industrial, information, operations, and cybersecurity).

3. USD(AT&L). The USD(AT&L):

a. Integrates policies established in this instruction and its supporting guidance into acquisition policy, regulations, and guidance consistent with DoDD 5134.01 (Reference (ar)).

b. Through the Assistant Secretary of Defense for Research and Engineering, monitors and oversees all DoD cybersecurity research and engineering investments, including research at the NSA.

- c. Integrates cybersecurity assessments into developmental testing and evaluation.
- d. Establishes and maintains the Cybersecurity and Information Assurance Center (formerly IA Technology Analysis Center) in accordance with DoDI 3200.12 (Reference (as)).
- e. Ensures that the DoD acquisition process incorporates cybersecurity planning, implementation, testing, and evaluation consistent with Reference (q), DoDI 8580.01 (Reference (at)), DoDD 5000.01 (Reference (au)), DoDI 5000.02 (Reference (av)), DoDI 4630.8 (Reference (aw)), section 1043 of Public Law 106-65 (Reference (ax)), and this instruction, in coordination with the DoD CIO.
- f. Assists with acquisition-related (e.g., research, development, test and evaluation (T&E)) agreements, and international cybersecurity and cyberspace defense negotiations and agreements, in accordance with Reference (ag), as needed.
- g. Ensures that PIT systems included in acquisition programs are designated, categorized, and have their authorization boundaries defined according to the guidelines provided in Reference (q).
- h. Ensures that policy and procedures for developing program protection plans (PPPs) required by DoDI 5200.39 (Reference (ay)) address cybersecurity in accordance with this instruction.
- i. Defines, develops, and integrates systems security engineering (SSE) into the systems engineering workforce and curriculum in accordance with DoDI 5134.16 (Reference (az)).
- j. Ensures that acquisition community personnel with IT development responsibilities are qualified in accordance with Reference (w) and DoD 8570.01-M (Reference (ba)).
- k. Coordinates with the DoD Test Resource Management Center (TRMC) for establishment of developmental T&E (DT&E) specific cybersecurity architectures and requirements.

4. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR DT&E (DASD(DT&E)). Under the authority, direction, and control of the USD(AT&L), the DASD(DT&E):

- a. Exercises oversight responsibility for developmental test planning in support of interoperability and cybersecurity for programs acquiring DoD IS and PIT systems in accordance with DoDI 5134.17 (Reference (bb)).
- b. Establishes procedures to ensure that cognizant DT&E authorities for acquisition programs verify that adequate DT&E to support cybersecurity is planned, resourced, documented, and can be executed in a timely manner prior to approval of program documents.

5. DOT&E. The DOT&E:

- a. Develops and provides policy for cybersecurity testing and evaluation during operational evaluations within DoD, including, but not limited to the DOT&E Memorandum (Reference (bc)) describing the cybersecurity testing process, clarified by updates in the DOT&E Memorandums (References (bd) and (be)).
- b. Conducts independent cybersecurity assessments during operational test and evaluation (OT&E) for systems under acquisition and reports the findings as part of the acquisition process.
- c. Oversees cybersecurity assessments by test agencies during both acquisition and exercise events as mandated by relevant statutory requirements.
- d. Reviews and approves cybersecurity OT&E documentation for all IT, IS, PIT, and special interest programs as required.

6. USD(P). The USD(P):

- a. Coordinates with the DoD CIO to ensure that cybersecurity strategies, policies, and capabilities are aligned with overarching DoD cyberspace policy, and are supportive of policies and capabilities relating to the disclosure of classified military information to foreign governments and international organizations in accordance with Reference (ab).
- b. Coordinates with the DoD CIO on international cybersecurity and cyberspace defense strategies and policies, as well as the negotiating, performing, and concluding agreements with international partners to engage in cooperative, international cybersecurity and cyberspace defense activities in accordance with Reference (af).
- c. Coordinates with the DoD CIO on enhancing DoD and DIB cyber situational awareness in accordance with Reference (ad) and in support of Reference (ae).

7. USD(P&R). The USD(P&R) supports implementation of cybersecurity requirements for effective manning, management, and readiness assessment of the cybersecurity workforce in accordance with References (w) and (ba).

8. USD(I). The USD(I):

- a. Coordinates with the DoD CIO on development and implementation of cybersecurity policy, guidance, procedures, and controls related to personnel, physical, industrial, information and operations security.

b. Coordinates with the DoD CIO and the USD(P) on intelligence-related international cybersecurity and cyberspace defense strategies, policies, and agreements with international partners.

c. Appoints the PAO for DoD ISs and PIT systems governed by the DoD portion of the Intelligence Mission Area (DIMA) as described in Reference (ac).

9. DIRNSA/CHCSS. Under the authority, direction, and control of the USD(I), and in addition to the cybersecurity-related responsibilities in DoDD 5100.20 (Reference (bf)) and the responsibilities in section 13 of this enclosure, the DIRNSA/CHCSS:

a. Supports the DoD CIO by providing cybersecurity architecture and mechanisms to support Defense military, intelligence, and business functions, including but not limited to cryptography, PKI, and IS security engineering services.

b. Evaluates or validates security implementation specifications described in this instruction.

c. Provides cybersecurity support to the DoD Components in order to assess threats to, and vulnerabilities of, information technologies.

d. Engages the cybersecurity industry and DoD user community to foster development, evaluation, and deployment of cybersecurity solutions that satisfy the guidance in this instruction.

e. Provides SSE services to the DoD Components, including describing information protection needs, properly selecting and implementing appropriate security controls, and assessing the effectiveness of system security.

f. Supports the development of NIST publications and provides engineering support and other technical assistance for their implementation within DoD.

g. Develops SSE training and qualification programs and oversees continuing education requirements for all trained IS security engineers and cybersecurity architects throughout DoD in accordance with Reference (ba).

h. Serves as the DoD focal point for the National IA Partnership and establishes criteria and processes for evaluating and validating all IA and IA-enabled products in accordance with CNSSP 11 (Reference (bg)).

i. Develops and issues security implementation specifications for the configuration of IA- and IA-enabled products (e.g., security configuration guides) and supports DISA in the development of SRGs and STIGs.

j. Serves as the DoD focal point for cybersecurity cryptographic research and development in accordance with Assistant Secretary of Defense for Research and Engineering direction and in coordination with the Director, Defense Advanced Research Projects Agency.

k. Manages the DoD IA Scholarship Program in accordance with sections 2200-2200f of Title 10, U.S.C. (Reference (bh)).

l. Plans, designs, manages, and executes the development and implementation of the key management infrastructure within DoD in coordination with DoD CIO.

m. Plans, designs, and manages the development and implementation of PKI within DoD, in coordination with DoD CIO and DISA.

n. Approves all applications of cryptographic algorithms for the protection of classified information.

o. Approves all cryptography used to protect classified information in accordance with CNSSP 15 (Reference (bi)).

p. Develops, implements, and manages a cybersecurity program for layered protection of DoD cryptographic SCI systems and a cybersecurity education, training, and awareness program for users and administrators of DoD cryptographic SCI systems in accordance with applicable DoD and DNI policies and guidance.

q. Conducts risk assessments of mobile code technologies, recommends the assignment of mobile code technologies to specific risk categories, and provides technical advice and assistance in the development of countermeasures to identified risks associated with specific mobile code technology implementations.

10. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 13 of this enclosure, the Director, DSS, monitors and oversees IS security practices of DoD contractors and vendors processing classified DoD information in accordance with DoD 5220.22M (Reference (bj)), and DoDD O-8530.1 (Reference (bk)), and DoDI O-8530.2 (Reference (bl)).

11. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 13 of this enclosure, the Director, DIA:

a. Provides finished intelligence, including threat assessments, in support of cybersecurity activities.

b. Develops, implements, and manages a cybersecurity program for DoD non-cryptographic SCI systems, including the DoD Intelligence IS (DoDIIS) and JWICS.

12. **DEPUTY CHIEF MANAGEMENT OFFICER (DCMO).** The DCMO appoints the PAO for DoD ISs and PIT systems governed by the Business Mission Area (BMA), as described in Section 2222 of Reference (aa).

13. **DoD COMPONENT HEADS.** The DoD Component heads:

- a. Ensure that IT under their purview complies with this instruction.
- b. Ensure that cybersecurity requirements are addressed and visible in all capability portfolios, IT life-cycle management processes, and investment programs incorporating IT.
- c. Appoint an AO for all DoD IS and PIT systems under their purview and ensure all DoD ISs and PIT systems are authorized in accordance with Reference (q).
- d. Ensure that PIT systems are identified, designated as such, and centrally registered at the DoD Component level.
- e. Ensure that SSE and trusted systems and networks (TSN) processes, tools, and techniques described in DoDI 5200.44 (Reference (bm)) are used in the acquisition of all applicable IT under their purview.
- f. Ensure that organizational solutions that support cybersecurity objectives acquired and developed via the ESSG process in accordance with Reference (aj) are implemented when possible, and participate in the ESSG process to ensure capabilities acquired or developed meet organizational requirements.
- g. Provide for a cybersecurity monitoring and testing capability in accordance with DoDI 8560.01 (Reference (bn)) and other applicable laws and regulations.
- h. Provide for vulnerability mitigation and incident response and reporting capabilities in order to:
 - (1) Comply with mitigations as directed by Commander, USSTRATCOM orders, or other directives such as alerts and bulletins and provide support to cyberspace defense, in accordance with Reference (bl).
 - (2) Limit damage and restore effective service following an incident.
 - (3) Collect and keep audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under their purview, and provide this data to appropriate law enforcement (LE) or other investigating agencies.
 - (4) Establish procedures to ensure prompt management action and reporting in accordance with:

(a) DoD Manual (DoDM) 5200.01, Volume 3 (Reference (bo)) for an actual or potential compromise of classified information.

(b) DoDM 5200.01, Volume 4 (Reference (bp)) for an actual or potential unauthorized disclosure of controlled unclassified information (CUI) (e.g., proprietary information, LE information).

(c) Reference (bj) when such losses occur on cleared contractor systems.

(d) DoD 5400.11-R (Reference (bq)) for a loss or unauthorized disclosure of personally identifiable information (PII) or other Privacy Act information.

(5) Comply with CNSS Instruction (CNSSI) 1010 (Reference (br)).

i. Ensure that contracts and other agreements include specific requirements to provide cybersecurity for DoD information and the IT used to process that information in accordance with this instruction.

j. Ensure that all personnel with access to DoD IT are appropriately cleared and qualified under the provisions of Reference (v) and that access to all DoD IT processing specified types of information (e.g., collateral, SCI, CUI) under their purview is authorized in accordance with the provisions of Reference (bo) and DoDM 5200.01, Volume 1 (Reference (bs)) or Reference (bp).

k. Ensure that personnel occupying cybersecurity positions are:

(1) Assigned in writing.

(2) Trained and qualified in accordance with References (w) and (ba).

(3) Assigned a position designation using the criteria found in Reference (v) and DoDI 1400.25 Vol. 731 (Reference (bt)). The position designation will be documented in the Defense Civilian Personnel Data System (DCPDS).

(4) Meet the associated suitability and fitness requirements,

l. Cybersecurity training and awareness products developed by DISA will be used to meet the baseline user awareness training required by Reference (w). DoD Components will provide additional cybersecurity orientation, training, and awareness programs to reinforce the objectives of the DoD Enterprise cybersecurity awareness programs to authorized users of ISs. This includes conducting additional in-depth training on DoD Component-specific topics.

m. Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing DoD Component-owned or controlled DoD ISs.

n. Ensure that cybersecurity solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities or access to or use of information and data by

individuals with disabilities in accordance with sections 791, 794, and 794d of Title 29, U.S.C. (Reference (bu)).

o. Conduct vulnerability assessments, Blue Team vulnerability evaluations and intrusion assessments, cybersecurity inspections, and Red Team operations (using internal or external capabilities) to provide a systemic view of enclave and IS cybersecurity posture.

p. Ensure that the cybersecurity testing and evaluation is conducted throughout the acquisition life cycle and integrated with interoperability and other functional testing, and that a cybersecurity representative participates in planning, execution, and reporting of integrated T&E activities as discussed in Enclosure 6 of Reference (av).

q. Collect and report cybersecurity metrics, and ensure that an annual assessment of the DoD Component cybersecurity program is conducted as required by section 3545 of Reference (aa).

r. Develop DoD IS contingency plans and conduct exercises to recover IS services following an emergency or IS disruption using guidance found in NIST SP 800-34 (Reference (bv)).

s. Establish a physical security program to protect DoD IT from damage, loss, theft, or unauthorized physical access in accordance with DoD 5200.08-R (Reference (bw)).

t. Ensure that all DoD ISs under their purview are registered in the DoD IT Portfolio Repository (DITPR) (at <https://ditpr.dod.mil/>) or the SIPRNET IT Registry (SITR) (at <http://dodcio.osd.smil.mil/itregistry>) in accordance with current DITPR and SITR guidance, or with the DoD Component SAP Central Office (SAPCO) for SAP ISs.

u. Ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs with any exceptions documented and approved by the responsible AO.

v. Establish a CD support element to coordinate CD activities with the UCDMO in accordance with DoD CIO Memorandum (Reference (bx)), and ensure transition from using CDSs on the UCDMO-managed CDS Sunset List to using CDSs on the UCDMO-managed CDS Baseline List.

w. Ensure use of the DISA-provided CD Services as the preferred method of addressing CD requirements.

x. Implement procedures issued by the DASD(DT&E) and DOT&E to ensure that cognizant T&E authorities for acquisition programs verify that adequate T&E support for cybersecurity requirements is planned, resourced, documented, and can be executed in a timely manner in accordance with References (bb), (bc), (bd), and (be).

y. Ensure individual and organization accountability within organizations under their purview, including:

(1) Hold commanders, IS owners (ISOs), AOs, information system security managers (ISSMs) (formerly known as IA managers), information system security officers (ISSOs), program managers (PMs), project and application leads, supervisors, and system administrators responsible and accountable for the implementation of DoD security requirements in accordance with this instruction, References (v), (bo), (bp), (bs), and (bw), DoDM 5200.01, Volume 2 (Reference (by)), DoD 5220.22-R (Reference (bz)), and supplemental DoD Component guidance. Personnel filling positions with privileged access must be qualified and sign a Statement of Acceptance of Responsibilities in accordance with Reference (ba).

(2) Ensure that military and civilian personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DoD information by not ensuring implementation of DoD security requirements in accordance with this instruction, other DoD 8500 series directives and instructions, DoD 5200 series instructions and publications, and supplemental DoD Component policies and procedures.

z. Ensure that requirements of CNSSP 300 (Reference (ca)), CNSSI 7000 (Reference (cb)), and other DIRNSA/CHNSS-issued guidance on compromising emanations (i.e., TEMPEST) are funded and implemented.

aa. Implement cybersecurity and cyberspace defense capabilities responsive to DoD requirements in accordance with Reference (bk) and (bl).

ab. Ensure that maintenance and disposal of information on DoD IT complies with the provisions of DoDD 5015.2 (Reference (cc)).

14. CJCS. In addition to the responsibilities in section 13 of this enclosure, the CJCS:

a. Provides advice and assessment on joint military requirements for cybersecurity assisted by the Joint Requirements Oversight Council in accordance with References (au) and (av).

b. Supports international cybersecurity and cyberspace defense activities of the DoD CIO.

c. Develops, coordinates, and promulgates cybersecurity policy, doctrine, and guidance for joint and combined operations consistent with this instruction, as required.

d. Appoints a PAO for DoD ISs and PIT systems governed by the Warfighting Mission Area as described in Reference (ac).

15. COMMANDER, USSTRATCOM. In addition to the responsibilities in section 13 of this enclosure, the Commander, USSTRATCOM:

a. Coordinates and directs DoD information networks operations and defense in accordance with the Unified Command Plan (Reference (cd)).

b. Ensures that Commander, USSTRATCOM orders addressing cybersecurity are consistent with the policy and guidance in this instruction and coordinated with the DoD CIO.

c. Chairs the DoD ISRMC and co-chairs the ESSG in accordance with References (aq) and (aj).

d. Oversees and ensures timely implementation of international cybersecurity and cyberspace defense agreements involving the geographic combatant commands.

e. Oversees DoD cybersecurity inspections as described in CJCSI 6510.01 (Reference (ce)) and operational risk assessments as described in NIST SP 800-30 (Reference (cf)) to maintain and determine compliance with security policy, procedures, and practices.

ENCLOSURE 3

PROCEDURES

1. INTRODUCTION

a. The purpose of the Defense cybersecurity program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DoD information, and to make choices based on that confidence.

b. The Defense cybersecurity program supports DoD's vision of effective operations in cyberspace where:

(1) DoD missions and operations continue under any cyber situation or condition.

(2) The IT components of DoD weapons systems and other defense platforms perform as designed and adequately meet operational requirements.

(3) The DoD Information Enterprise collectively, consistently, and effectively acts in its own defense.

(4) DoD has ready access to its information and command and control channels, and its adversaries do not.

(5) The DoD Information Enterprise securely and seamlessly extends to mission partners.

c. In accordance with DoDD 5105.53 (Reference (cg)), the Director of Administration and Management is responsible for providing policy, oversight, direction, and control, including exercise of the authorities of the Secretary of Defense pursuant to chapter 159 of Reference (bh), for the management, operation, security, protection, safety, renovation, construction, and IT of the Pentagon Reservation and supported DoD facilities and space in the National Capital Region, including the Raven Rock Mountain Complex and alternate sites.

2. RISK MANAGEMENT

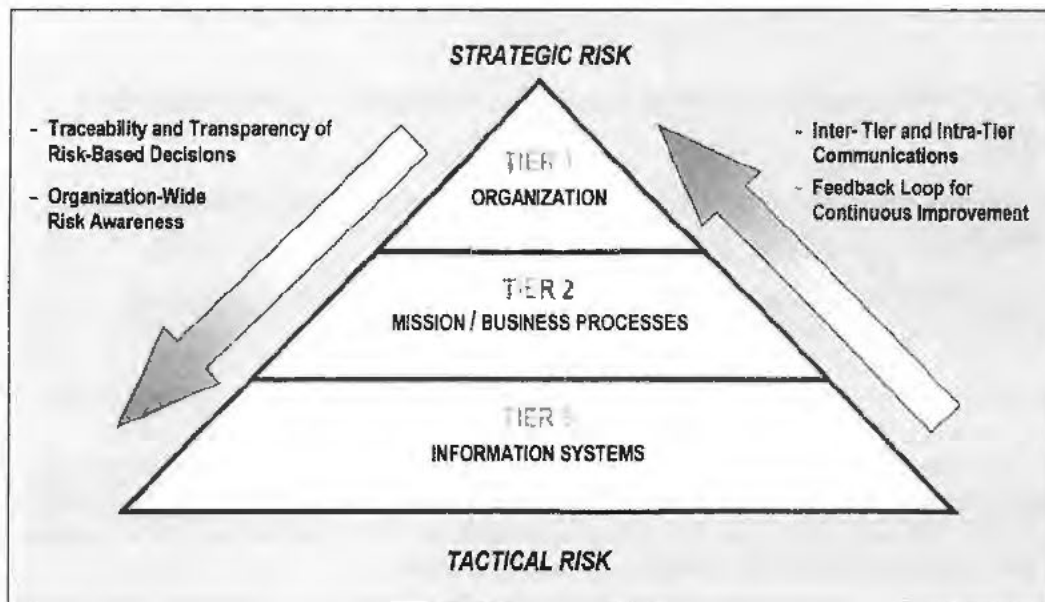
a. Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (av), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.

(1) DoD will use NIST SP 800-37 (Reference (ch)), as implemented by Reference (q), to address risk management, including authorization to operate (ATO), for all DoD ISs and PIT systems.

(2) DoD IS and PIT systems will transition to CNSSI 1253 (Reference (ci)), NIST SP 800-53 (Reference (cj)), and Reference (ch) in accordance with transition guidance provided in Reference (q).

b. **Integrated Organization-Wide Risk Management.** Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization as described in Reference (o). Figure 1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at the organization level, the mission and business process level, and the IS level.

Figure 1. Three-Tiered Approach to Risk Management



(1) Risk management at Tier 1 addresses risk from an organizational perspective. As part of the feedback loop, Tier 1 risk management is informed and influenced by risk decisions made in Tiers 2 and 3.

(a) A comprehensive IS security governance structure is established that provides assurance that IS security strategies are aligned with and support mission and business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility.

(b) The DoD ISRMC, comprising the four MA PAOs and other major DoD and IC stakeholders, provides the Tier 1 risk management governance for DoD.

(2) Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1, and informed and influenced by risk decisions made in Tier 3.

(a) The activities at Tier 2 begin with the design, development, and implementation of the mission and business processes defined at Tier 1.

(b) The PAOs for each DoD MA provide the Tier 2 governance for their respective MAs.

(3) Tier 3 addresses risk from an IS and PIT system perspective and is guided by the risk decisions at Tiers 1 and 2.

(a) Though the need for specific protections is identified at Tiers 1 and 2, it is at Tier 3 where the information protections are applied to the system and its environment of operation for the benefit of successfully enabling mission and business success.

(b) Information protection requirements are satisfied by the selection and implementation of appropriate security controls in Reference (cj). Security controls are implemented at Tier 3 by common control providers, system managers (SMs), or PMs, and risk-based authorization decisions are granted by AOs.

c. Risk Management in the System Development Life Cycle

(1) Risk management tasks begin early in the system development life cycle and are important in shaping the security capabilities of the IS. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development life cycle, the tasks will, by necessity, be undertaken later in the life cycle and will be more costly and time consuming to implement, and could negatively impact the performance of the IS.

(2) Cybersecurity risk management is planned for and documented in a cybersecurity strategy (formerly known as IA strategy) in accordance with References (at) and (av), and included in the PPP for all acquisition programs. Periodic reviews of the PPP and associated systems engineering documents should evaluate the status of cybersecurity solutions as part of the larger systems development.

(3) Risk management must continue during operations and sustainment. This may include the application of new or revised security controls prior to the integration of new IT services or products into an existing operational IS in order to maintain the security of the operational IS.

d. DoD ISRMC. The DoD ISRMC, supported by the DSAWG, is the DoD risk executive function as described in References (o) and (ch).

e. Risk Management Framework (RMF). DoD uses Reference (ch) as implemented by Reference (q), and is applicable to all DoD ISs and PIT systems. The RMF provides a disciplined and structured process that combines IS security and risk management activities into

the system development life cycle and authorizes their use within DoD. The RMF has six steps: categorize system; select security controls; implement security controls; assess security controls; authorize system; and monitor security controls.

f. Risk Assessment. Risk assessment is a key step in the organizational risk management process. Risk assessments will be performed in accordance with the process in Reference (cf) and as described on the Knowledge Service (KS) (i.e., recommending preferred risk assessment approaches and analysis approaches). In particular, all of the risk factors described in Reference (cf) must be used across components and agencies of the DoD to ensure reciprocity and ease of sharing risk information. The robustness of the risk assessments may be tailored to accommodate resource constraints and the availability of detailed risk factor information (e.g., threat data); however, any tailoring must be clearly explained in risk assessment reports to ensure that AOs understand to what degree they can rely on the results of the risk assessments.

g. Security Controls. Security controls are expressed in a specified format (e.g., a control number, a control name, control text, and enhancement text).

(1) All DoD IS and PIT systems will be categorized in accordance with Reference (ci) and will implement a corresponding set of security controls that are published in Reference (cj) regardless of whether they are National Security System (NSS) or non-NSS.

(2) All security controls used by DoD are published in the security control catalog in Reference (cj), with supporting validation procedures in NIST 800-53A (Reference (ck)).

(3) DoD-specific assignment values, implementation guidance, and validation procedures will be developed by the DoD CIO with direct support from NSA/CSS and DISA and input from the other DoD Components and will be published in the KS at <https://diacap.iaportal.navy.mil>.

(4) The DoD CIO, with direct support from NSA/CSS and DISA, and input from the other DoD Components, works with NIST to ensure that the security control catalog remains up-to-date and continues to represent DoD needs.

(5) Detailed guidance on DoD IS and PIT system categorization and security control selection is provided in Reference (q).

h. Cybersecurity Reciprocity

(1) Within DoD, reciprocity has been implemented as cybersecurity reciprocity to differentiate it from the application of reciprocity to other disciplines. Cybersecurity reciprocity reduces time and resources wasted on redundant test, assessment and documentation efforts.

(2) Cybersecurity reciprocity is best achieved through transparency (i.e., making sufficient evidence regarding the security posture of an IS or PIT system available, so that an AO from another organization can use that evidence to make credible, risk-based decisions regarding the acceptance and use of that system or the information it processes, stores, or transmits). DoD

Components must share security authorization packages with affected information owners (IOs) or stewards and interconnected ISOs to support cybersecurity reciprocity. The reciprocal acceptance of DoD and other federal agency and department security authorizations will be implemented in accordance with the procedures in Reference (q).

3. OPERATIONAL RESILIENCE. Operational resilience requires three conditions to be met: information resources are trustworthy; missions are ready for information resources degradation or loss; and network operations have the means to prevail in the face of adverse events. Operational resilience must be achieved by:

a. Using TSN requirements and best practices to protect mission-critical functions and components and manage risks to the integrity of critical information and communications technology in accordance with Reference (bm) for the sustainment of IT. This includes the use of criticality analysis, all-source threat informed acquisition, and engineering mitigations, and the authorities prescribed in section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Reference (cl)). TSN processes and best practices must be applied early and across the system development life cycle, and be applied to system acquisitions and the purchase and integration of replacement IT as described in Reference (bm).

b. Performing developmental T&E of cybersecurity in accordance with Reference (av) and OT&E in accordance with References (bc) and (bd), including the ability to detect and react to penetrations and exploitations and to protect and restore data and information, in order to inform acquisition and fielding decisions.

c. Supporting acquisition program protection by:

(1) Ensuring cybersecurity is a key element of program protection planning activities that manage risks to advance technology and mission-critical system functionality from foreign collection due to design vulnerability or supply chain exploit insertion, and battlefield loss throughout the system life cycle.

(2) Having mission criteria for identifying critical components and critical program information as established in References (bm) and (ay).

d. Planning for mission continuation in the face of degraded or unavailable information resources in accordance with DoDD 3020.26 (Reference (cm)), and integrating those plans and priorities into the DoD Information Enterprise.

e. Exercising under realistic cyber conditions and testing procedures and tactics for work-arounds and fall-backs in the face of hostility in accordance with Secretary of Defense Memorandum (Reference (cn)). This includes:

(1) Conducting periodic exercises or evaluations of the ability to operate during loss of all information resources and connectivity.

(2) Being able to allocate information resources dynamically as needed to sustain mission operations while addressing cyber failures, no matter the cause.

(3) Being able to restore information resources rapidly to a trusted state while maintaining support to ongoing missions.

f. Preserving the trust in the security of DoD information during transmission.

(1) Transmission of DoD information must be protected through the communications security (COMSEC) measures and procedures established in DoDI 8523.01 (Reference (co)) and security controls that support transmission security (TRANSEC) in Reference (cj).

(2) COMSEC monitoring and cybersecurity readiness testing will be conducted in accordance with Reference (bn).

(3) Compromising emanations (i.e., TEMPEST) countermeasures must be applied in accordance with policy in Reference (ca), guidance in Reference (cb), and other TEMPEST guidance as issued by the DIRNSA/CHCSS.

g. Using automation whenever possible in support of cybersecurity objectives including, but not limited to, secure configuration management, continuous monitoring, active cyber defense, and incident reporting and situational awareness.

4. INTEGRATION AND INTEROPERABILITY

a. Net-Centric Operations. A net-centric model provides people, services, and platforms the ability to discover one another and connect to form new capabilities or teams without being constrained by geographic, organizational, or technical barriers. The net-centric model allows people, services, and platforms to work together to achieve shared ends. To be net-centric, cybersecurity will be designed, organized, and managed such that it can work together in any combination that events demand and maintain an expected level of readiness so that all required cybersecurity assets can be brought to bear in a rapid and flexible manner to meet new or changing mission needs.

b. Integration. Cybersecurity must be fully integrated into system life cycles so that it will be a visible element of organizational, joint, and DoD Component architectures, capability identification and development processes, integrated testing, information technology portfolios, acquisition, operational readiness assessments, supply chain risk management, SSE, and operations and maintenance activities.

c. Interoperability

(1) Cybersecurity products (e.g., firewalls, file integrity checkers, virus scanners, intrusion detection systems, anti-malware software) should operate in a net-centric manner to enhance the exchange of data and shared security policies.

(2) Semantic, technical, and policy interoperability will be used to integrate disparate cybersecurity products into a net-centric enterprise that can work together to create new intelligence and make and implement decisions at network speed.

(3) Semantic, technical, and policy interoperability support products are designed to provide security for communications between different IT systems. Interoperable communications must be consistent with approved cryptographic design and current system implementation standards. The objective is to ensure the seamless and secure exchange of classified or sensitive information that is critical to the success of DoD mission goals and objectives.

d. Standards-Based Approach. The DoD cybersecurity and cyberspace defense data strategy will enable semantic, technical, and policy interoperability through a standards-based approach that has been refined by many in industry, academia, and government. It is an information-oriented approach (see for example the security content automation protocol (SCAP) discussion in NIST SP 800-126 (Reference (cp))).

e. DoD Architecture Principles. Interoperability and effective management of security content will be achieved through adherence to DoD cybersecurity architectures as issued. All DoD Components must commit to these architectures to facilitate sharing of information necessary to achieve mission success while managing the risk inherent in interconnecting systems.

f. Knowledge Repositories. These contain a broad collection of best practices, benchmarks, standards, templates, checklists, tools, guidelines, rules, principles, and the like. Examples include the National Vulnerability Database (<http://nvd.nist.gov/>), the Open Vulnerability and Assessment Language Repository (<http://oval.mitre.org/repository/>), and the DoD's KS as defined in Reference (q). In many respects, knowledge repositories serve as the cybersecurity and cyberspace defense community "memory" and they enable policy or process interoperability and should be used to share information and answer questions.

5. CYBERSPACE DEFENSE. Cyberspace defense uses architectures, cybersecurity, intelligence, counterintelligence (CI), other security programs, LE, and other military capabilities to harden the DoD Information Enterprise to be more resistant to penetration and disruption; to strengthen the U.S. ability to respond to unauthorized activity and defend DoD information and networks against sophisticated and agile cyber threats; and to recover quickly from cyber incidents.

a. Defense of DoD IT. Defense of DoD IT and information networks is under the direction of the Commander, USSTRATCOM, in accordance with Reference (cd) and is conducted as described in Commander, USSTRATCOM, orders or other directives such as alerts and bulletins, Reference (bl), and DoD Manual O-8530.01 (Reference (cq)). Cyberspace defense is integrated with other elements of network operations as described in DoDI 8410.02 (Reference (cr)).

b. Continuous Monitoring Capability. DoD will establish and maintain a continuous monitoring capability that provides cohesive collection, transmission, storage, aggregation, and presentation of data that conveys current operational status to affected DoD stakeholders. DoD Components will achieve cohesion through the use of a common continuous monitoring framework, lexicon, and workflow as specified in NIST SP 800-137 (Reference (cs)).

c. Penetration and Exploitation Testing. Evaluation of cybersecurity during an acquisition T&E event must include independent threat representative penetration and exploitation testing and evaluation of the complete system cyberspace defenses including the controls and protection provided by computer network defense service providers. Penetration and exploitation testing must be planned and resourced as part of the DT&E and OT&E via the appropriate program test documentation.

d. Cyber Defense Personnel. Cyber defense personnel operating on or in DoD IS will be identified using identity authentication methods in DoDI 8520.03 (Reference (ct)).

e. LE and CI (LE/CI)

(1) The DoD Cyber Crime Center, as described in DoDD 5505.13 (Reference (cu)), provides digital and multimedia forensics and specialized cyber investigative training and services. In this role it coordinates and facilitates relationships across LE, intelligence, and homeland security communities.

(2) DoD component LE/CI agencies deploy capabilities on DoD networks with the intent to identify and investigate the human element posing a threat to DoD IT and DoD information. Cybersecurity will be used in support of countering espionage, international terrorism, and the CI insider threat in accordance with DoDI 5240.26 (Reference (cv)).

(3) DoD network administrators will accommodate all applicable legitimate and lawful deployment of LE/CI tools and solutions. DoD LE/CI organizations in turn will make all reasonable attempts to coordinate the implementation of LE/CI solutions with their respective AO in a manner consistent with service-level change control processes in order to avoid any disruption to mission critical operational tempo.

f. Insider Threat. Insider threats must be addressed in accordance with policy and procedures published by the USD(P).

6. PERFORMANCE

a. Organizations will implement processes and procedures to accommodate three conditions necessary to realize effective cybersecurity that is consistently implemented across DoD:

(1) Organization Direction. This includes organizational mechanisms for establishing and communicating priorities and objectives, principles, policies, standards, and performance

measures.

(2) A Culture of Accountability. This includes aligning internal processes, maintaining accountability, and informing, making, and following through on decisions with implications for cyberspace protection and defense.

(3) Insight and Oversight. This includes measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity implementation and reporting across all organizations without impeding local missions.

b. In addition to the structures that facilitate DoD's major decision processes (e.g., the Joint Chiefs of Staff Joint Capabilities Integration and Development System described in CJCSI 3170.01 (Reference (cw)), DoDD 7045.14 (Reference (cx)), Reference (au)) cybersecurity performance is facilitated by the DoD CIO Executive Board in accordance with the DoD CIO Memorandum (Reference (cy)) and its supporting governance bodies (e.g., IA Senior Leadership forum, DoD ISRMC).

c. Strategic cybersecurity metrics will be defined, collected, and reported by the DoD CIO in partnership with the DoD Components. DoD CIO will develop and issue guidance regarding how cybersecurity metrics are determined, established, defined, collected, and reported.

7. DoD INFORMATION

a. The DoD Information Security Program is described in DoDI 5200.01 (Reference (cz)). All classified information and CUI must be protected in accordance with References (bs), (by), (bo), and (bp).

b. DoD's information sharing policies and procedures are defined in DoDD 8320.02 (Reference (da)) and DoD 8320.02-G (Reference (db)). Information sharing actions and activities will be aligned with the DoD Information Sharing Operational Strategy and Guidance (see www.dodcio.defense.gov). A security clearance held is an attribute of any identified DoD person, and that attribute should be discovered and considered when a decision is made to share classified information. If the information intended to be shared is not classified, then other attributes associated with the identity of the sharing recipient may need to be discovered before the sharing is executed.

c. The Defense cybersecurity program provides the mechanisms to measure, monitor, and enforce information security and sharing policies and procedures as they relate to information in an electronic form, primarily through the implementation of security controls.

d. Information systems must protect classified information and CUI from unauthorized access by requiring authentication in accordance with Reference (ct) prior to making an access decision.

e. All unclassified DoD information that has not been cleared for public release in accordance with DoDD 5230.09 (Reference (dc)) and that is in the possession or control of non-DoD entities on non-DoD ISs must be protected in accordance with DoDI 8582.01 (Reference (dd)).

f. Classified information and export controlled unclassified information released or disclosed to industry in connection with contracts under the National Industrial Security Program must be protected in accordance with Reference (bj).

g. Spillage of classified information onto an unclassified IS, of higher-level classified information onto a lower level classified IS, or of classified information onto an IS not authorized to the appropriate level must be handled in accordance with Reference (bo).

h. To enable automated sharing and protection, all DoD information must include marking and metadata as required by References (bp), (bs) and (da), and that information must be in the format specified in References (bp) and (by).

i. DoD IT that processes or stores PII or protected health information must comply with Reference (bq), DoDI 5400.16 (Reference (de)), and DoD 8580.02-R (Reference (df)).

j. In accordance with Reference (de), a privacy impact assessment (PIA) is required for DoD ISs that collect, maintain, use, or disseminate PII about members of the public, federal personnel, contractors, or foreign nationals (FNs) employed at U.S. military facilities internationally.

k. All non-DoD entities that process unclassified DoD information on non-DoD ISs, to the extent provided by the applicable contract, grant, or other legal agreement or understanding with DoD, must comply with applicable Defense Federal Acquisition Regulation Supplements and will comply with Reference (dd), and, if a cleared contractor, with Reference (bj).

l. Unclassified DoD information in the possession of the DIB will be protected by conducting DIB cybersecurity as established in Reference (ad), and cleared contractor facilities will be protected in accordance with Reference (bj).

m. Cryptography required to protect DoD information will be implemented in accordance with Reference (bi).

n. DoD information proposed or projected for publication on public Internet media (e.g., website, blog, social media) must be reviewed and approved for public dissemination in accordance with Reference (dc), DoD Manual 5205.02 (Reference (dg)), and DoDI 8550.01 (Reference (dh)).

8. IDENTITY ASSURANCE

a. Identity assurance ensures strong identification and authentication, and eliminates anonymity in DoD ISs so that entities' access and access behavior are visible, traceable, and

enable continuous monitoring for LE and cybersecurity. Person and non-person entity identity policies, standards, information, infrastructure, issuance, and revocation processes and procedures that bind the physical and digital representations of entities will incorporate measures to ensure the integrity, authenticity, security, privacy, and availability of authoritative identity information across the full spectrum of DoD mission environments and operations.

(1) DoD ISs will use only DoD-approved identity credentials to authenticate entities requesting access to or within the Defense information environment. This requirement extends to all mission partners using DoD ISs.

(2) The identification of entities accessing DoD ISs must be recorded in order to deny anonymity and deter abuse of authorized IS access. DoD will implement capabilities to record, track, and monitor specific entity access to networks, applications, and web servers.

b. DoD IS will employ identity assurance procedures that are aligned with the DoD Identity Management Strategic Plan and the Identity Assurance Implementation Guidance and Roadmap to the extent practical.

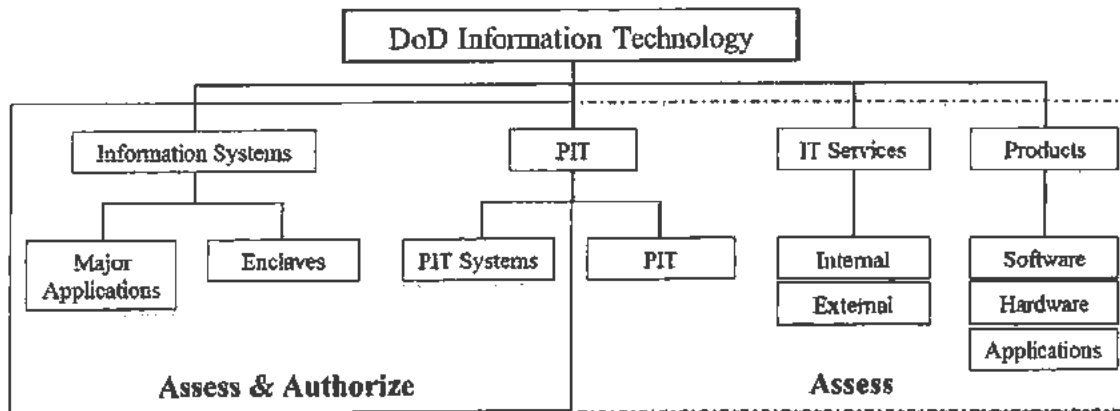
c. Information and infrastructure that support identity reliant functions, processes, and procedures used in support of DoD operations, including but not limited to identity credentialing, will incorporate measures to ensure the confidentiality, integrity, authenticity, and availability of identity data or identity credentials.

d. Identity assurance policies and procedures regarding identity authentication for ISs are in Reference (ct).

9. INFORMATION TECHNOLOGY

a. IT. Cybersecurity applies to all IT that receives, processes, stores, displays, or transmits DoD information, as shown in Figure 2.

Figure 2. DoD Information Technology



(1) **Information Systems.** Cybersecurity requirements must be identified and included in the design, development, acquisition, installation, operation, upgrade, or replacement of all DoD ISs in accordance with section 3544 of Reference (aa), References (q) and (r), section 2224 of Reference (bh), this instruction, and other cybersecurity-related DoD guidance, as issued.

(a) DoD ISs are typically organized in one of two forms:

1. Enclave

a. Enclaves provide standard cybersecurity, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

b. Enclaves always assume the highest security category of the ISs that they host, and derive their security needs from those systems. See Reference (ch) for a discussion of IS boundaries and the application of security controls.

2. Major Application (Formerly Automated Information System Application)

a. Certain applications, because of the information in them, require special management oversight due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application and should be treated as major applications. A major application may be a single software application (e.g., integrated consumable items support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Enrollment Eligibility Reporting System).

b. Major applications include any application that is a product or deliverable of an Acquisition Category I through III program as defined in Enclosure 3 of Reference (av). When operationally feasible all new major applications will be hosted in a Defense Enterprise Computing Center.

g. All applications, regardless of whether they rise to the level of major application or not, require an appropriate level of protection. Adequate security for other than major applications may be provided by security of the environment in which they operate.

d. When possible, capabilities should be developed as applications hosted in existing authorized computing environments (i.e., enclaves) rather than designated as major applications requiring new and separate authorizations.

e. DoD Component CIOs will resolve disputes regarding whether an application rises to the level of a major application.

(b) DoD IS Registration. All DoD ISs will be registered in the DITPR (at <https://ditpr.dod.mil/>) or the SITR (at <http://dodcio.osd.smil.mil/itregistry>) in accordance with current DITPR and SITR guidance, or with the DoD Component SAPCO for SAP ISs. New DoD ISs should be entered into the DITPR or SITR at the beginning of the system development life cycle.

(c) Stand-Alone Systems. DoD ISs and PIT systems that are stand-alone must be authorized to operate, but assigned security control sets may be tailored as appropriate with the approval of the AO (e.g., network-related controls may be eliminated).

(d) Notice and Consent Banners. Standard mandatory notice and consent banners must be displayed at logon to all ISs and standard mandatory notice and consent provisions will be included in all DoD IS user agreements in accordance with applicable security controls and DoD implementation procedures in the KS. Official DoD standard notice and consent language will be posted on the KS with copies posted to the IASE.

(2) PIT

(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (q) for PIT cybersecurity requirements.

(b) Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste

water, natural gas and steam), telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).

(c) Cybersecurity requirements must be identified, tailored appropriately, and included in the acquisition, design, development, developmental and operational testing and evaluation, integration, implementation, operation, upgrade, or replacement of all DoD PIT in accordance with References (bm) and (ay), this instruction, and other cybersecurity-related DoD guidance, as issued.

(d) Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a collection of PIT rises to the level of a PIT system.

1. PIT systems are analogous to enclaves but are dedicated only to the platforms they support. PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

2. All DoD PIT systems will be categorized as defined in Reference (ci) and authorized in accordance with Reference (q).

3. Although other federal departments and agencies may treat PIT systems as a type of IS, DoD platforms supporting certain DoD missions have unique operational and security needs. Due to the specialized purpose of their application, PIT systems require uniquely tailored security control sets and control validation procedures and require security control assessors and AOs with specialized qualifications.

4. Interconnections between PIT systems and other PIT systems or DoD ISs must be protected either by implementation of security controls on the PIT system or the DoD IS.

5. For PIT systems that are stand-alone, assigned security control sets may be tailored as appropriate with the approval of the AO (e.g., network-related controls may be eliminated).

6. PIT systems must be registered at the DoD Component level.

(3) **IT Service.** An IT service is a form of a DoD internet service as described in Reference (dh). It consists of IT capabilities that are provided according to a formal agreement between DoD entities or between DoD and an entity external to DoD. Capabilities may include, for example, information processing, storage, or transmission.

(a) An IT service is provided from outside the authorization boundary of the organizational IS using the IT service and the using organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

(b) IT services are net-centric and may be provided over service oriented or cloud computing architectures and may be Internet-based.

(c) An internal IT service is implemented within DoD. The DoD entity providing the service is responsible for the application of appropriate security controls and for ensuring that ISs supporting service delivery are assessed and authorized in accordance with Reference (q). Service-level agreements (SLAs) will be executed for internal services.

(d) An external IT service is implemented outside DoD. The DoD entity using the external service will:

1. Ensure that interagency agreements or government statements of work for external services incorporate requirements in accordance with this instruction. Requirements for external services must include the application of appropriate security controls to the IT supporting the external service delivery in accordance with Reference (q). Requests for proposals will include sufficient information on which to evaluate each offeror's proposed approach to satisfying the security control requirements.

2. Ensure that processes, roles, and responsibilities are established between program management office and network operations entities for continued assessment.

3. Ensure that all security relevant and operational status changes are reported through the organization's network operations chain of command to the Commander, USSTRATCOM.

4. DoD enterprise-level agreements for services should be used when possible.

(4) IT Product

(a) Unified capability products will receive unified capability certification for cybersecurity in accordance with Reference (ao).

(b) Products that protect classified information must comply with Reference (bg).

(c) Products must meet security configuration guidance in accordance with Chapter 113 of Reference (s) and comply with the connection approval process established in Reference (am).

(d) Products will comply with the requirements of Reference (bm), as applicable.

b. IT Considerations. These are general considerations that apply to IT.

(1) All acquisitions of DoD IS will comply with Reference (at) and USD(AT&L) Memorandum (Reference (di)).

(2) SMs and PMs must use TSN tools, techniques, and practices, including the use of all-source threat assessments to inform acquisition and engineering mitigation decisions, for all IT when required in accordance with Reference (bm). During sustainment, TSN practices will be applied prior to integrating IT into operational IS.

(3) Cybersecurity will be implemented in all system and service acquisitions at levels appropriate to the system characteristics and requirements throughout the entire life cycle of the acquisition in accordance with Reference (q).

(4) All acquisitions of qualifying IT must have an adequate and appropriate cybersecurity strategy that will be reviewed prior to acquisition milestone decisions and acquisition contract awards in accordance with References (at), (av), and Section 811 of Public Law 106-398 (Reference (dj)) and must plan for developmental test oversight by DASD(DT&E) and operational test oversight by DOT&E.

(5) Each mobile code technology used in DoD information systems must undergo a risk assessment, be assigned to a mobile code risk category, and have its use regulated based on its potential to cause damage to DoD operations and interests if used maliciously.

(6) Ports, protocols, and services will be managed in accordance with Reference (an).

(7) DoD use of space systems will follow cybersecurity policy established in DoDI 8581.01 (Reference (dk)).

(8) Disposal and destruction of classified hard drives, electronic media, processing equipment components, and the like will be accomplished in accordance with Reference (bo), CNSSI 4004.1 (Reference (dl)), and applicable security controls.

(9) Disposal of unclassified electronic media will be accomplished in accordance with the guidelines provided in NIST SP 800-88 (Reference (dm)) and applicable security controls.

(10) Cryptographic products used to protect IT and the information that resides in the IT will be acquired and implemented in accordance with Reference (bi).

(11) All IA products and IA-enabled products that require use of the product's IA capabilities will comply with the evaluation and validation requirements of Reference (bg).

(12) All IT will be assigned to and governed by a DoD Component cybersecurity program.

(13) IT below the system level (i.e., IT services and products) will be security configured and reviewed by the cognizant ISSM (under the direction of the AO) for acceptance and connection into an authorized computing environment (i.e., an IS enclave with an ATO).

(14) Cybersecurity must be consistent with enterprise architecture principles and guidelines within the DoD Architecture Framework (Reference (dn)) and DoD cybersecurity architectures developed or approved by the DoD CIO.

(15) Connections to the DISN must comply with connection approval procedures and processes as established in Reference (am).

(16) The ESSG will oversee development and acquisition of enterprise solutions for use throughout DoD that support cybersecurity objectives in accordance with Reference (aj).

(17) All persons entrusted with the management of DoD IT will be responsible for proper use, care, physical protection, and disposal or disposition in accordance with DoDI 5000.64 (Reference (do)), DoDI 2030.02 (Reference (dp)) and, when appropriate, Reference (bo).

(18) In addition to complying with the provisions of DoDI 1035.01 (Reference (dq)):

(a) Telework solutions involving the use of DoD-owned, government-furnished equipment for remote access to unclassified DoD networks will comply with the requirements of applicable security controls defined in Reference (cj).

(b) Telework solutions involving the use of non-government furnished equipment (i.e., any computer or other telework device not furnished by DoD) for remote access to unclassified DoD networks will be developed by the DoD Components desiring the capability based on the guidance provided in NIST SP 800-114 (Reference (dr)) and evaluated and approved by the DoD CIO on a case-by-case basis.

(19) Basic input and output systems (BIOSs) will be managed in accordance with Section 3.2 of SP 800-147 (Reference (ds)). Specifications for personal computer client systems must include the requirement for BIOS protections compliant with Section 3.1 of Reference (ds).

(20) In anticipation of emerging trusted platform module (TPM) product capabilities, as well as requirements for device identification, authentication, encryption, measurement, and device integrity, DoD Components will ensure new computer assets (e.g., server, desktop, laptop, thin client, tablet, smartphone, personal digital assistant, mobile phone) procured to support DoD will include a TPM version 1.2 or higher where required by DISA STIGs and where such technology is available.

(a) Vendor TPMs must be in conformance with Trusted Computing Group standards (www.trustedcomputinggroup.org/groups/tpm) and must be approved by the procuring DoD Component. The TPM must be turned on and ready for provisioning when the computer asset is received from the vendor. Written justification must be provided to the responsible AO if assets are procured without TPM technology in cases where it is available.

(b) DIRNSA will identify use cases and implementation standards and plans for DoD to leverage TPM functionality fully to enhance IT device security, including platform integrity

verification (BIOS firmware and operating system software), platform identification and authentication, and enhanced encryption (hardware based key generation and certificate and key storage).

(21) DoD IT must comply with SCAP standards established in Reference (cp). STIGs developed by DISA will use SCAP standards.

(22) All use of Internet-based capabilities will comply with References (bp), (dc), (dg), and (dh).

(23) As the NIST and CNSS publications change, the impact of those changes will be incorporated into the KS.

(24) All DoD IT that is designated as an NSS must comply with CNSS policy issuances.

10. CYBERSECURITY WORKFORCE

a. The DoD IA Workforce Improvement Program develops and maintains a trained and qualified cybersecurity workforce by providing a continuum of learning from basic literacy to advanced skills, recruiting and retaining highly qualified professionals, and keeping workforce capabilities current in the face of constant change as described in References (w) and (ba).

b. All cybersecurity personnel must be assigned in writing to identified cybersecurity positions, and trained and qualified in accordance with References (w) and (ba).

c. All authorized users of DoD IS must receive initial cybersecurity awareness orientation as a condition of access and, thereafter, participate in both DoD's and their Component's enterprise cybersecurity awareness program.

d. Cybersecurity functions, as defined in Reference (ba), that may be performed by non-U.S. citizens, non-DoD personnel, contractors, or non-U.S. service providers will be so identified.

e. All cybersecurity positions will be assigned a position designation using the criteria found in References (v) and (bs) and will meet the associated suitability and fitness requirements. The position designation will be documented in the DCPDS. Non-U.S. citizens may not serve as ISSMs, as ISSOs, in supervisory cybersecurity positions, or be responsible for PKI certificate issuance. Non-U.S. citizens may serve as system administrators and perform maintenance on cybersecurity enabled products provided they are under the immediate supervision of a U.S. citizen and meet the investigative requirements of Reference (v).

11. MISSION PARTNERS

a. Integral to the success of the Defense cybersecurity program is the promotion of systems and communications interoperability and advancement of operational cybersecurity and

cyberspace defense relationships with all mission partners at both the unclassified and classified levels; integration of cybersecurity and cyberspace defense activities with mission partner critical infrastructure protection initiatives; and creating cybersecurity and cyberspace defense training and exercise opportunities to build mission partner operational capacity, improve global cyber situational awareness, and develop a collective global cybersecurity and cyberspace defense workforce. This will be accomplished through the planning, negotiation, and implementation of cybersecurity and cyberspace defense agreements with mission partners.

b. DoD will operate a PKI for use by foreign national (FN) mission partners to communicate with Combatant Commands that will enable use of digital signature, encryption, and PKI-based authentication and be implemented and operated in accordance with DoD Coalition Public Key Infrastructure, X.509 Certificate Policy (Reference (dt)).

c. Foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD ISs containing classified or sensitive information only if these conditions are met:

(1) Access to DoD ISs is authorized only by the DoD Component head in accordance with DoD, Department of State, and ODNI disclosure guidance, as applicable.

(2) Mechanisms are in place to limit access strictly to information that has been cleared for release to the represented foreign nation, coalition, or international organization (e.g., North Atlantic Treaty Organization) in accordance with Reference (ab) for classified military information, and other policy guidance for unclassified information such as References (bp), (dp), DoDD 5230.20E (Reference (du)), and DoDI 5230.27 (Reference (dv)).

d. Capabilities built to support cybersecurity objectives that are shared with mission partners will be governed through integrated decision structures and processes described in this instruction, must have formal agreements (e.g., a memorandum of agreement, memorandum of understanding, SLAs, contracts, grants, or other legal agreements or understandings) that incorporate considerations for DoD risks, be in accordance with Reference (am), and will be consistent with applicable guidance contained in References (ab), (bo), (bp), (bu), (bs), (by), and DoDI 2040.02 (Reference (dw)).

e. Information systems jointly developed by DoD and mission partners are considered DoD-partnered systems. The cybersecurity risk management considerations for DoD-partnered systems are provided in Reference (q).

f. Agreements with international partners to engage in cooperative international cybersecurity activities must be formally negotiated and concluded in accordance with Reference (ag), and any associated classified military information will be released only in accordance with Reference (ab).

g. The release of cryptographic national security systems technical security material, information, and techniques to foreign governments or international organizations must be approved by the CNSS in accordance with Reference (ak).

12. DoD SISO. On behalf of the DoD CIO, the DoD SISO:

- a. Directs and coordinates the Defense cybersecurity program and, as delegated, carries out the DoD CIO's responsibilities pursuant to section 3544 of Reference (aa).
- b. Serves as the DoD CIO's primary liaison to DoD AOs, ISOs, and ISSOs.
- c. Advises, informs, and supports DoD PAOs and their representatives.
- d. Ensures that DoD IT is assigned to and governed by a DoD Component cybersecurity program.
- e. Maintains liaison with DNI CIO to ensure continuous coordination of DoD and IC cybersecurity activities and programs.
- f. Maintains liaison with NIST to ensure continuous coordination and collaboration on NIST cybersecurity-related issuances.
- g. Provides guidance and oversight in the development, submission, and execution of the DoD cybersecurity program budget and advocates for DoD-wide cybersecurity solutions throughout the planning, programming, budget, and execution process.
- h. Develops guidance regarding how cybersecurity metrics are determined, established, defined, collected, and reported.
- i. Collects and reports cybersecurity metrics in coordination with the DoD Component heads as required by section 3545 of Reference (aa).
- j. Coordinates with USD(AT&L) to integrate cybersecurity concepts into the DoD acquisition process by:
 - (1) Supporting the USD(AT&L) in ensuring the DoD acquisition process incorporates cybersecurity planning, implementation, and testing consistent with References (p), section 3544 of (aa), (q), (af), (av), and this instruction.
 - (2) Supporting the USD(AT&L) in its acquisition oversight of major defense acquisition programs, major automated ISs, or other programs of special interest that are, or include, IT, by:
 - (a) Providing subject matter experts to participate in AT&L oversight of system engineering technical reviews and the review of system engineering artifacts to ensure that cybersecurity requirements are incorporated early and that the implementation of those requirements is maturing across the acquisition life cycle.
 - (b) Informing USD(AT&L) of acquisition program risk related to a failure to address cybersecurity requirements in accordance with this policy.

k. Coordinates with the DOT&E to ensure cybersecurity testing and evaluation is integrated into the DoD acquisition process in accordance with References (bc), (bd), and other DOT&E policies and guidance.

l. Coordinates with USD(P) to ensure cybersecurity policies related to disclosure of classified military information to foreign governments and international organizations is in accordance with Reference (af) and (ab).

m. Provides recommended updates and additions to NIST for security controls that are published in Reference (cj) and for supporting validation procedures published in Reference (ck) with direct support from NSA/CSS and DISA, and input from the other DoD Components.

n. Provides recommended updates and additions to the security control baselines and overlays that are published in Reference (ci) and used by DoD with direct support from NSA/CSS and DISA, and input from the other DoD Components.

o. Develops DoD-specific assignment values, implementation guidance, and validation procedures for Reference (cj) security controls and publishes them in the KS at <https://diacap.iaportal.navy.mil> with direct support from NSA/CSS and DISA, and input from the other DoD Components.

p. Ensures that organization-wide solutions that support cybersecurity objectives acquired and developed via the ESSG process in accordance with Reference (aj) are consistent with DoD architecture, policy, and guidance developed by the DoD CIO to ensure solutions acquired or developed meet organizational requirements.

q. Manages international cybersecurity and cyberspace defense activities and represents DoD in carrying out assigned international cybersecurity and cyberspace defense responsibilities and functions through the International Cybersecurity Program.

r. Manages and executes DoD DIB Cybersecurity and IA Program activities in accordance with Reference (ad).

13. DoD COMPONENT CIOs. DoD Component CIOs:

a. On behalf of the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program that is consistent with the strategy and direction of the DoD SISO and the Defense cybersecurity program, and compliant with this instruction.

b. Appoint DoD Component SISOs to direct and coordinate their DoD Component cybersecurity program.

c. When code signing certificates are used to establish provenance of software code, implement a process to designate individuals authorized to receive code-signing certificates and ensure that such designations are kept to a minimum consistent with operational requirements.

d. Partner with DoD Component Acquisition Executives to ensure that all IT is acquired in accordance with DoD cybersecurity policy and that program risk relating to the development of cybersecurity requirements is assessed, communicated to the Milestone Decision Authority and managed early in the system development life cycle.

14. DoD RISK EXECUTIVE FUNCTION. The risk executive function, as described in Reference (ch), is performed by the DoD ISRMC. The DoD risk executive:

a. Ensures risk-related considerations for individual ISs and PIT systems, including authorization decisions, are viewed from a DoD-wide perspective with regard to the overall strategic goals and objectives of DoD in carrying out its missions and business functions.

b. Ensures that management of IT-related security risks is consistent across DoD, reflects organizational risk tolerance, and is considered along with other organizational risk in order to ensure mission or business success.

15. PAO. PAOs:

a. Oversee and establish guidance for the strategic implementation of cybersecurity and risk management within their MAs.

b. Appoint flag-level (e.g., general officer, senior executive) PAO representatives to, and to oversee, the DoD ISRMC.

c. Assist the DoD CIO and DoD SISO in assessing the effectiveness of DoD cybersecurity.

16. AO. AOs:

a. Ensure that:

(1) For DoD ISs and PIT systems under their purview, cybersecurity-related positions are identified in their organization's manpower structure in accordance with References (w), (ba), and DoDI 1100.22 (Reference (dx)).

(2) Appointees to cybersecurity-related positions are given a written statement of cybersecurity responsibilities.

(3) ISSMs meet all requirements specified in Reference (v).

- b. Render authorization decisions for DoD ISs and PIT systems under their purview in accordance with Reference (q).
- c. Establish guidance for and oversee IS-level risk management activities consistent with Commander, USSTRATCOM, and DoD Component guidance and direction.
- d. Must be U.S. citizens and DoD officials with the authority to assume responsibility formally for operating DoD ISs or PIT systems at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

17. ISOs of DoD IT. ISOs of DoD IT:

- a. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.
- b. Ensure that SSE is used to design, develop, implement, modify, and test and evaluate the system architecture in compliance with the cybersecurity component of the DoD Enterprise Architecture (as described in Reference (r)) and to make maximum use of enterprise cybersecurity.
- c. Ensure authorized users and support personnel receive appropriate cybersecurity training.
- d. Coordinate with the DoD Component TSN focal point to ensure that TSN best practices, processes, techniques, and procurement tools are applied prior to the acquisition of IT or the integration of IT into ISs when required in compliance with Reference (bm).

18. ISSM. ISSMs:

- a. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.
- b. Ensure that IOs and stewards associated with DoD information received, processed, stored, displayed, or transmitted on each DoD IS and PIT system are identified in order to establish accountability, access approvals, and special handling requirements.
- c. Maintain a repository for all organizational or system-level cybersecurity-related documentation.
- d. Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.

e. Monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring.

f. Ensure that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.

g. Ensure implementation of IS security measures and procedures, including reporting incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures in accordance with Reference (bo) for classified information or Reference (bp) for CUI, respectively.

h. Ensure that the handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with Reference (bo).

i. Act as the primary cybersecurity technical advisor to the AO for DoD IS and PIT systems under their purview.

j. Ensure that cybersecurity-related events or configuration changes that may impact DoD IS and PIT systems authorization or security posture are formally reported to the AO and other affected parties, such as IOs and stewards and AOs of interconnected DoD ISs.

k. Ensure the secure configuration and approval of IT below the system level (i.e., products and IT services) in accordance with applicable guidance prior to acceptance into or connection to a DoD IS or PIT system.

19. INFORMATION SYSTEM SECURITY OFFICER (ISSO) (formerly known as IA Officers). When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles. ISSOs:

a. Assist the ISSMs in meeting their duties and responsibilities.

b. Implement and enforce all DoD IS and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documentation.

c. Ensure that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before being granted access to those systems.

d. In coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO.

e. Ensure that all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals.

20. PRIVILEGED USERS. Privileged users (e.g., system administrators) must:

a. Configure and operate IT within the authorities vested in them according to DoD cybersecurity policies and procedures.

b. Notify the responsible ISSO or, in the absence of an ISSO, the responsible ISSM, of any changes that might affect security posture.

21. AUTHORIZED USERS. Authorized users must:

a. Immediately report all cybersecurity-related events (e.g., data spill) and potential threats and vulnerabilities (e.g., insider threat) to the appropriate ISSO or, in the absence of an ISSO, the ISSM.

b. Protect authenticators commensurate with the classification or sensitivity of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

c. Protect terminals, workstations, other input or output devices and resident data from unauthorized access.

d. Inform the responsible ISSO when access to a particular DoD IS or PIT system is no longer required (e.g., completion of project, transfer, retirement, resignation).

e. Observe policies and procedures governing the secure operation and authorized use of DoD IT, including operations security in accordance with Reference (dg) and DoDD 5205.02E (Reference (dy)).

f. Use DoD IT only for official or authorized purposes.

g. Not unilaterally bypass, strain, or test cybersecurity mechanisms. If cybersecurity mechanisms must be bypassed, users will coordinate the procedure with the ISSO and receive written approval from the ISSM.

h. Not introduce or use software, firmware, or hardware that has not been approved by the AO or a designated representative on DoD IT.

i. Not relocate or change DoD IT equipment or the network connectivity of equipment without proper authorization.

j. Meet minimum cybersecurity awareness requirements in accordance with Reference (ba).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	authorizing official
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ATO	authorization to operate
BIOS	basic input and output system
BMA	Business Mission Area
CCI	control correlation identifier
CD	cross-domain
CDS	cross-domain solution
CI	counterintelligence
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	communications security
CSS	Central Security Service
CUI	controlled unclassified information
DASD(DT&E)	Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
DCMO	Deputy Chief Management Office
DCPDS	Defense Civilian Personnel Data System
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
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

DITPR	DoD Information Technology Portfolio Repository
DNI	Director of National Intelligence
DoD CIO	DoD Chief Information Officer
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	DoD directive
DoDI	DoD instruction
DoDIIS	DoD Intelligence Information System
DoDM	DoD manual
DOT&E	Director, Operational Test and Evaluation
DSAWG	Defense Information Assurance Security Accreditation Working Group
DSS	Defense Security Service
DT&E	Developmental Test and Evaluation
DTM	directive-type memorandum
EIEMA	enterprise information environment mission area
ESSG	Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group
FN	foreign national
GIG	Global Information Grid
IA	information assurance
IASE	information assurance support environment
IC	Intelligence Community
IO	information owner
IS	information system
ISO	information system owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
KS	Knowledge Service

LE	law enforcement
LE/CI	law enforcement and counterintelligence
MA	mission area
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security System
OT&E	operational test and evaluation
PAO	principal authorizing official
PIA	privacy impact assessment
PII	personally identifiable information
PIT	platform information technology
PKI	public key infrastructure
PM	program manager
PPP	program protection plan
RMF	risk management framework
SAP	special access program
SAPCO	SAP Central Office
SCAP	security content automation protocol
SCI	sensitive compartmented information
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer
SITR	Secret Internet Protocol Router Network Information Technology Registry
SLA	Service-level agreement
SM	system manager
SP	Special Publication
SRG	security requirements guide
SSE	system security engineering
STIG	security technical implementation guide

T&E	test and evaluation
TPM	trusted platform module
TRANSEC	transmission security
TRMC	Test Resource Management Center
TSN	trusted systems and networks
UCDMO	Unified Cross Domain Management Office
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSTRATCOM	United States Strategic Command

PART II. DEFINITIONS

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

application. Defined in Reference (dz).

authenticator. Defined in Reference (dz).

authorized user. Defined in Reference (w).

availability. Defined in Reference (dz).

Blue Team. Defined in Reference (dz).

CCI. Decomposition of an NIST control into single, actionable, measurable statement.

confidentiality. Defined in Reference (dz).

continuous monitoring. Defined in Reference (cs).

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. (Reference (m))

cybersecurity architect. See "Information Security Architect" definition in Reference (ch).

cyberspace. Defined in Reference (dz).

cyberspace defense. Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate.

DoD-controlled. Used only for DoD purposes, dedicated to DoD processing, and effectively under DoD configuration control.

DoD information. Any information that has not been cleared for public release in accordance with Reference (dc) and that has been collected, developed, received, transmitted, used, or stored by DoD, or by a non-DoD entity in support of an official DoD activity.

DoD Information Enterprise. Defined in Reference (r).

DoD IS. DoD-owned IS and DoD-controlled IS. A type of DoD IT.

DoD IT. DoD-owned IT and DoD-controlled IT. DoD IT includes IS, PIT, IT services, and IT products.

DoD-partnered systems. 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).

FN. Defined in Joint Publication 1-02 (Reference (ea)).

enclave. Defined in Reference (dz).

GIG. Defined in Reference (r).

identity assurance. See “assurance” definition in NIST SP 800-63 (Reference (eb)).

IA. Defined in Reference (dz).

IA and IA-enabled product. Defined in Reference (bg).

IQ. Defined in Reference (dz).

information resource. Defined in Reference (dz).

information steward. Defined in Reference (dz).

insider threat. Defined in Reference (cv).

integrity. Defined in Reference (dz) as NIST SP 800-53 definition.

IS. Defined in Reference (dz).

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

IS security engineer. Defined in Reference (dz).

ISSM. Defined in Reference (dz).

ISSO. Defined in Reference (dz).

IT. Defined in Reference (dz).

IT product. Individual IT hardware or software items. Products can be commercial or government provided and include, but are not limited to, operating systems, office productivity software, firewalls, and routers.

IT Service. A capability provided to one or more DoD entities by an internal or external provider based on the use of information technology and that supports a DoD mission or business process. An IT Service consists of a combination of people, processes, and technology.

key management infrastructure. Defined in Reference (dz).

major application. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Reference (al))

MA. Defined in Reference (ac).

mission partners. Defined in Reference (r).

mobile code. Defined in Reference (dz).

mobile code risk categories. Categories of risk associated with mobile code technology based on functionality, level of access to workstation, server, and remote system services and resources, and the resulting threat to information systems.

NSS. Defined in Reference (dz).

network. Defined in Reference (dz).

operational resilience. The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

overlay. Defined in Reference (ci).

PIA. Defined in Reference (de).

PIT. IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

PIT system. A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

policy interoperability. Common business processes related to the transmission, receipt, and acceptance of data among participants.

privileged user. Defined in Reference (dz).

private DoD internet service. Defined in Reference (dh).

PM or SM. The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.

PPP. Defined in Reference (ay).

public key enabling. Defined in Reference (dz).

reciprocity. Defined in Reference (dz).

Red Team. Defined in Reference (dz).

risk executive function. Defined in Reference (dz).

security category. Defined in Reference (dz).

security control assessor. Defined in Reference (ch).

security controls. Defined in Reference (dz).

security posture. Defined in Reference (dz).

semantic interoperability. The ability of each sending party to communicate data and have receiving parties understand the message in the sense intended by the sending party.

SISO. See “Senior (Agency) Information Security Officer” definition in Reference (ch). The SISO role, as described in law (Reference (aa)) and by NIST, should not be confused with information security roles and responsibilities within References (bo), (bp), (bs), (by), and (cz).

SRG. Compilation of CCI groups in more applicable, specific technology areas at various levels of technology and product specificity. Contain all requirements that have been flagged as applicable from the parent level regardless if they are selected on a DoD baseline or not.

SSE. See “IS security engineering” definition in Reference (dz).

stand-alone system. System that is not connected to any other network and does not transmit, receive, route, or exchange information outside of the system’s authorization boundary.

STIG. Based on DoD policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

supply chain risk. Defined in Reference (bm).

system development life cycle. Defined in Reference (dz).

technical interoperability. The ability for different technologies to communicate and exchange data based on well-defined and widely adopted interface standards.

TEMPEST. Defined in Reference (dz).

TRANSEC. Defined in Reference (dz).

TPM. The TPM is a microcontroller that stores keys, passwords, and digital certificates. It typically is affixed to the motherboard of computers. It potentially can be used in any computing device that requires these functions. The nature of this hardware chip ensures that the information stored there is made more secure from external software attack and physical theft. The TPM standard is a product of the Trusted Computing Group consortium. For more information on the TPM specification and architecture, refer to www.trustedcomputinggroup.org/groups/tpm.

UCDMO CDS Baseline List. A list managed by the UCDMO that identifies CDSs that are available for deployment within the DoD and IC.

UCDMO CDS Sunset List. A list managed by the UCDMO that identifies CDSs that are or have been in operation but are no longer available for additional deployment and need to be replaced within a specified period of time.



SNLC



Quarterly Program Review Sep 4-5 FT Detrick, MD Final Version



U.S. ARMY



unclass conf bridge 301-878-2000 passcode 298



Introductions

9/4 - 9/5 FINAL Attendees List

DISA

1 Mr. [REDACTED]	Chief, Senior National Leadership Communications Division (OPC/ [REDACTED])	[REDACTED]@mail.mil	(301) 225-4751/4800
2 Mr. [REDACTED]	Electronics Engineer, Senior National Leadership Communications [REDACTED]	[REDACTED]@mail.mil	(301) 225-2106
Mr. [REDACTED]	Deputy, Senior National Leadership Communications Division (OPC [REDACTED])	[REDACTED]@mail.mil	(301) 225-2681

MOLINK

5 LTC [REDACTED]	Chief MOLINK and Senior Presidential Translator	[REDACTED]mil@mail.mil	(703) 697-9240
6 MCPO [REDACTED]	JS Navy, Senior Presidential Communicator, Washington-Moscow [REDACTED]	[REDACTED]mil@mail.mil	(703) 697-9240

JSP

7 Mr. [REDACTED]	DCL/SNLC Advisor	[REDACTED]civ@mail.mil	(703) 545-8017
8 Mr. [REDACTED]	Joint Service Provider (JSP) DCL/SNLC Technical Advisor	[REDACTED]civ@mail.mil	(703) 614-6604

White House

9 Mr. [REDACTED]	WHCA	[REDACTED]@whmo.mil	(202) 757-6719
------------------	------	---------------------	----------------

State Department

10 Mr. [REDACTED]	Division Chief, SMO	[REDACTED]@state.gov	(202) 634-0208
11 Mr. [REDACTED]	Branch Chief, NRRC	[REDACTED]@state.gov	(202) 647-7779
12 [REDACTED]	Communications Officer, NRRC	[REDACTED]@state.gov	(202) 647-0380

FT Detrick

13 Mr. [REDACTED]	Chief Executive Officer, USASA-Detrack	[REDACTED]@mail.mil	(301) 619-3604
14 Mr. [REDACTED]	Operations Chief, USASA-Detrack	[REDACTED]@mail.mil	(301) 619-3601
15 Mr. [REDACTED]	Senior Linguist, USASA-Detrack	[REDACTED]@mail.mil	(301) 619-2818
16 Mr. [REDACTED]	Maintenance Chief, USASA-Detrack	[REDACTED]@mail.mil	(301) 619-2160
17 Mr. [REDACTED]	Brigade DCoS, 21st Signal Brigade	[REDACTED]civ@mail.mil	(301) 619-6191
Mr. [REDACTED]	Civilian Executive Officer / Chief Information Officer	[REDACTED]civ@mail.mil	(301) 619-6831

ISEC

18 Mr. [REDACTED]	ISEC Team Lead	[REDACTED]v@mail.mil	(520) 538-3365
19 CPT [REDACTED]	Outgoing ISEC Team Lead	[REDACTED]park.mil@mail.mil	(520) 454-1065
20 Mr. [REDACTED]	Computer Engineer	[REDACTED]civ@mail.mil	(520) 454-1057

PdM WESS

21 Mr. [REDACTED]	Project Officer, Satellite Terminal Systems (STS)	[REDACTED].mil	(703) 806-4874
22 Mr. [REDACTED]	Project Lead & COR	[REDACTED]ail.mil	(571) 358-0622
23 Mr. [REDACTED]	Assistant Project Lead	[REDACTED]v@mail.mil	(443) 395-9649
24 Mr. [REDACTED]	Project Coordinator	[REDACTED]ctr@mail.mil	(703) 806-8512

SEC

25 Ms. [REDACTED]	Software Engineer, Software Engineering Center	[REDACTED]@mail.mil	(443) 395-6074
26 Mr. [REDACTED]	IT Specialist (Sys Admin), Software Engineering Center	[REDACTED]civ@mail.mil	(443) 395-5982
27 Mr. [REDACTED]	IT Specialist (Sys Admin), Software Engineering Center	[REDACTED]@mail.mil	(443) 395-6021

UNCLASSIFIED//FOUO



Due-Outs



ID	Due Out Description	Owner	Suspense
1	Prepare for Nov 19-21 Tech Meeting (extension dates 16-23)	DISA	18-Nov-19
	-Modernization Risks, Timeline, Decision & Implementation brief/discussion	ISEC CPT Park	NLT 10 Sep
	-Implement CCB/WorkGroup 29 Oct 2019 (1 day) - WHCA	DISA	NLT 28 Oct
2	Classification Guide or Guidance	DISA	TBD
	-Identify owner for this classification guide	DISA Willie Stephens	TBD
	-State Department - Ned will provide State Dept guidance & email guidance to Travis & John	State Dept Ned Williams	NLT 13 Sep 2019
3	RMF	DISA	TBD
	-Submit for RMF Approving Official (AO) Mr. Greenwell for the SNLC Program	DISA Willie Stephens	NLT 13 Sep 2019
	-Schedule DISA or NSA Assessment for FT Detrick	DISA Willie Stephens	NLT 13 Sep 2019
	-Submit for RMF certification for antenna (assumption DISA AO and 302nd/ASA as operators)	WESS John Myung	TBD
4	Submit CCB Charter for JSAP (Joint Staff Action Procedure) for CIO G6 and all stakeholders	WESS John Myung	NLT 13 Sep 2019
5	DISA (or is it G6) funding for commercial and lease line	DISA Willie Stephens	Next QPR
6	MOLINK IT Desktop/Servers Hand Receipt	WESS John Myung	NLT 13 Sep 2019
	-WESS picks up on HR & xfer to MOLINK		
7	SNLC Trados SIPR sharefolder for all user stakeholders	DISA Eng Sofiane Oumsa	31-Oct
8	SIPR sharefolder for general SNLC stakeholders	DISA Eng Sofiane Oumsa	31-Oct
9	CHAT system	SEC James Roach	TBD
	-23-26 Sep ISEC/SEC/MOLINK validation	WESS John Myung	5-Sep-19
	-Project Master Schedule w Definition	SEC James Roach	NLT 13 Sep 2019
10	Solarwinds Requirements Review and project schedule for CCB Review	SEC James Roach	NLT 20 Sep 2019
11	Ticketing Requirements and project schedule for CCB Review	SEC James Roach	NLT 27 Sep 2019



QPR Agenda

4 Sep

- 1000 – 1200
1. Introductions & QPR Ground Rules
 2. References
 3. Stakeholders w/ Roles & Responsibilities
 4. Annual Battle Rhythm Events
 5. Modernization Timeline
 6. Control Configuration Board (CCB)
- 1300 – 1600
7. SNLC Network “As-Is”

5 Sep

- 1000 -1600
8. SNLC Network “To-Be”
 9. Due Outs



Ground Rules

1. Be Accountable, Be Frank and Be Professional
2. During the Network “As-Is”/ Network “To-Be” Discussions -
 - a) Focus on current requirements
 - b) Exceptions:
Lessons learned/best practices or effects current requirements
3. Keep discussions at the Unclass//FOUO
 - a) Do not use US site name/location – instead use organizations or “T”
 - b) Do not discuss operations



References

2 of 2



2009 OASD-NII
Oversight NLCC

4. OASD (NII)/CIO Oversight (28 APR 2009)

- a) Discusses DISA COMSEC Responsibilities
- b) References CIO Responsibilities



2012 CCB Charter

5. Control Configuration Board CCB Charter (18 May 2012)

- a) Defines the x2 oversight groups (CCB & CCB Advisory), Workgroups (Standing/Ad Hoc, Engineering/Software), and CCB related roles/responsibilities
- b) Assigns CIO G6/Chief for LandWarNet Integration Division serves as the Configuration Manager and Chairman of the CCB
- c) Discusses Standing Sub-Committee for Upgrades (SSU)
- d) Unsigned and needs to be updated



2018 MTE

6. Meeting of Technical Experts (27-29 November 2018)

- a) Section 2 & 3 reviews 01 Oct 17 – 30 Sep 18 for SCS (DCL, DVL, CL), Daily Service Messages, Foreign Affairs Link (FAL), America-Russia-UK (ARUK), Modernization Proposal, Nuclear Risk Reduction Center (NRRC), Military Communications Link (MCL); background, performance, recommendations
- b) Signed protocols
- c) References CIO responsibilities



US Stakeholders Roles and Responsibilities:



DISA SNLC

1 of 2

1. Assigned as the US Competent Agency responsible to implement 2008 Secure Communications System (SCS) Agreement:
 - a) Determine the configuration and technical parameters of the comms circuits, encryption devices, and equipment to be used
 - b) Provide for the maintenance, continuous operation, and security of the SCS
 - c) Develop recommendations & operating procedures for the SCS
 - d) Review and resolve issues regarding changes to configuration and operations mode
2. Plan, Schedule and Implement nation-level Working Groups, Meeting of Technical Experts, Quarterly Program Review and other meetings as necessary (SCS 2.D.1)
3. Designated to establish, operate, & maintain SNLC COMSEC account (ASD(NII)/DoD CIO 28 Apr 2009)
4. Programming and funding of commercial, leased lines (CIO G6)
5. Exercise program management and technical oversight of all activities pertaining to the SNLC and DCL UTCP systems.



US Stakeholders Roles and Responsibilities:



DISA SNLC

2 of 2

6. Chair the CCB Advisory Council and coordinate activities of the CCB with organizations external to the CCB.
7. Provide the CCB information on overall program concerns and agreements that apply to or have impact on the SNLC programs.
8. 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 the Senior National Leadership Communications (SNLC) network.
9. Work closely with PM DCATS to ensure all new requirements or anticipated upgrades are adequately budgeted.
10. Provide COMSEC materiel required to all sites in order for them to perform their roles and responsibilities in the shared Operation & Maintenance (O&M), management and upgrades of the SNLC Network.
11. Provide overall program COMSEC CM. This effort includes updating cryptographic equipment software or coordinating with various cryptographic equipment holders to ensure the software is updated. All agencies with program related laboratory or experimental crypto equipment are expected to comply if DISA requests that lab tests be conducted with new crypto software prior to deployment.



US Stakeholders Roles and Responsibilities:



CIO G6

1 of 1

1. DCL Configuration Control Board (CCB) Chairman:

- a) Notify the board members of scheduled meetings.
- b) Convene the board in formal session on at least a quarterly basis, or as required, for the resolution/coordination of significant issues concerning the DCL system.
- c) Assure the resolution of all change proposals submitted for review and action. Represent the Army at SSU meetings in the absence the Director of Architectures, Operations, Networks, and Space in the CIO/G6.
- d) Ensure all proposed changes are properly documented and processed for evaluation by the CCB.
- e) Implement all other actions deemed necessary by the CCB to maintain an effective and coordinated CM program.

2. References:

- a) OASD/C3I Memo, dated 28 Jul 2000, confirming Army as the Lead Military Department (LMD) for life cycle management, procurement, installation, operation, training, maintenance, supply support, PPBES responsibilities
- b) AR 25-1, The Army Information Resources Management Program, dated 15 July 2005, directs the CIO/G-6 to provide oversight for National Security Systems (NSS) over Army information systems and other DOD systems for which the Army has been given responsibility, including the DCL program



US Stakeholders Roles and Responsibilities:



MOLINK

1 of 1

1. At their option, provide Tier 1 UTCP support, receiving telephone or on site assistance from NISO or other support element as necessary
2. At their option, provide Tier 1 SNLC support, receiving telephone or on site assistance from NISO or other support element as necessary
3. Immediately notify NISO of all SNLC outages
4. Assist NISO in keeping up to date records of hardware including serial numbers, nomenclature and location
5. Assist NISO by furnishing trouble ticket information as necessary
6. Identify individuals within MOLINK who are willing and able to participate in all or some of the Tier 1 support efforts. The extent of the Tier 1 efforts performed by MOLINK will be determined by MOLINK. Tier 1 support individuals in MOLINK should periodically review the UTCP restoral procedures, the UTCP drawing package and SNLC documentation.
7. Develop a schedule for periodically testing restoral equipment by applying UTCP restoral procedures. This periodic testing should also be used as training, by assigning the restoral procedures to individuals in need of hands on experience. These training experiences should be proctored by more experienced individuals to ensure accuracy. They should also be monitored by others in need of training to enhance the efficacy of the training opportunity.

Reference: 2009 MOA for SNLC



US Stakeholders Roles and Responsibilities:



WHCA

1 of 1

1. Provide Tier 1 UTCP support, receiving telephone or on site assistance from NISO as necessary
2. Provide Tier 1 SNLC support, receiving telephone or on site assistance from NISO as necessary
3. Immediately notify NISO or PTCF (as delineated in NISO documentation) of all SNLC outages
4. Contact the JSEC help desk as needed
5. Provide 72 hours notice prior to scheduled maintenance outages and 24 hours notice for demand maintenance outages
6. Assume responsibility for COMSEC at their location and coordinate with DISA for the proper destruction of superseded COMSEC material
7. Assist NISO in keeping up to date records of hardware including serial numbers, nomenclature and location
8. Assist NISO by furnishing trouble ticket information as necessary
9. Assist NISO with keeping off line equipment antivirus definitions updated, if necessary
10. Be responsible for all property at their location

Reference: 2009 MOA for SNLC



US Stakeholders Roles and Responsibilities:



State Department

1 of 1

1. Provide Tier 1 and Tier 2 UTCP support, receiving telephone or on site assistance from JSEC as necessary
2. Provide Tier 1 SNLC support, receiving telephone or on site assistance from NISO as necessary
3. Immediately notify NISO or PTCF (as delineated in NISO documentation) of all SNLC outages
4. Contact the JSEC help desk as needed
5. Provide 72 hours notice prior to scheduled maintenance outages and 24 hours notice for demand maintenance outages
6. Assume responsibility for COMSEC at their location and coordinate with DISA for the proper destruction of superseded COMSEC material
7. Assist NISO in keeping up to date records of hardware including serial numbers, nomenclature and location
8. Assist NISO by furnishing trouble ticket information as necessary
9. Assist NISO with keeping off line equipment antivirus definitions updated, if necessary
10. Be responsible for all property at their location

Reference: 2009 MOA for SNLC



US Stakeholders Roles and Responsibilities:

Network Infrastructure Services & Opns (NISO)

1 of 4

- Provide Tier 1 support to MOLINK
- Provide Tier 1 support to all locations, including site visits (Tier 1 support will begin with local support personnel)
- Provide Tier 1 and Tier 2 SNLC network support
- Provide SNLC network management on a 24/7/365 basis. Serve as liaison between the Pentagon TCF and SNLC customers to ensure SNLC support that involves the Pentagon TCF is effective. Document and disseminate to all customers the correct procedures for employing Pentagon TCF and/or NISO DCL support.
- Provide a single document to MOLINK, State Department and other customers providing contact procedures for all support available from Pentagon local support
- Maintain and disseminate up-to-date POC information for all telecommunications equipment locations
- Provide SNLC network preventive and demand maintenance and operational checks
- Provide complete SNLC Configuration Management, including equipment, cabling, documentation and system database
- Fund SNLC equipment repairs
- Fund SNLC software releases



US Stakeholders Roles and Responsibilities:

Network Infrastructure Services & Opns (NISO)

2 of 4

- Fund and maintain a Tier 3 Promina support contract
- Coordinate scheduled maintenance outages with DISA, MOLINK and SNLC locations (as applicable) at least 72 hours in advance
- Coordinate demand maintenance outages with DISA, MOLINK and SNLC locations (as applicable) at least 72 hours in advance
- Maintain the skills required to duplicate a hard drive using the “ntbackup” and Automatic System Recovery (ASR) procedure.
- Provide hard drive backups using the ASR procedure when/if requested by customers
- Be responsible for COMSEC in the Pentagon and coordinate with DISA for the proper destruction of superseded COMSEC material
- Request assistance from JSEC as necessary
- Assist DISA with requests for service (RFS), Telecommunications Service Requests (TSR) and Telecommunications Service Orders (TSO)
- Assist MOLINK (if requested by MOLINK) with MOLINK’s efforts to periodically test equipment by performing restoral procedures
- Track and coordinate resolution of problems and provide outage notification and status updates to Army GNOSC and JTF-GNO



US Stakeholders Roles and Responsibilities:

Network Infrastructure Services & Opns (NISO)

3 of 4

- Coordinate with telecommunications vendors to ensure system availability of 99.99% or better
- Update off line equipment antivirus definitions at the Pentagon and assist with the updates at other locations (may require travel to those locations)
- Recognize that telecommunications links will cause most UTCP and SNLC problems and plan/prioritize manpower and hours of operation accordingly
- Complete DISA and PM DCATS technical input requests concerning current and future SNLC network equipment and links
- Prepare supplemental operations and maintenance documentation that reflects NISO support experiences
- Provide and maintain a trouble ticket system (or set up an account with an existing Pentagon trouble ticket system)
- Complete a trouble ticket for *all* actions related to UTCP and SNLC support, including NISO actions and those performed by MOLINK and sites
- Cover as many office hours per week as feasible with cross-trained technicians
- Ensure all technicians are capable of all Tier 1 services across SNLC and UTCP systems (cross train and take turns at like tasking to ensure all technicians remain competent in all areas)



UNCLASSIFIED//FOUO

US Stakeholders Roles and Responsibilities:



ASA, 302nd Sig Bn, 21st Signal Brigade

1 of 1

- Provide Tier 1 UTCP support, receiving telephone or on site assistance from NISO as necessary
- Provide Tier 1 SNLC support, receiving telephone or on site assistance from NISO as necessary
- Immediately notify NISO or PTCF (as delineated, in NISO documentation) of all SNLC outages
- Contact the JSEC help desk as needed
- Provide 72 hours notice prior to scheduled maintenance outages and 24 hours notice for demand maintenance outages
- Assume responsibility for COMSEC at their location and coordinate with DISA for the proper destruction of superseded COMSEC material
- Assist NISO in keeping up to date records of hardware including serial numbers, nomenclature and location
- Assist NISO by furnishing trouble ticket information as necessary
- Assist NISO with keeping off line equipment antivirus definitions updated, if necessary
- Be responsible for all property at their location

Reference: 2009 MOA for SNLC



UNCLASSIFIED//FOUO

US Stakeholders Roles and Responsibilities:



PdM WESS

1 of 1

1. Assists the Army in carrying out its DCL Executive Agency mission for DOD by acquiring any new or upgraded DCL system.
2. PM DCATS is responsible for the overall acquisition and installation of all communications sub-systems managed by the CCB, which are approved by the SSU in response to changes in user requirements.
3. Project funding for procurements associated with this program will be managed by PM-DCATS. PM DCATS can further delegate its acquisition responsibilities to one of its subordinate Product Managers as necessary.
4. The PM will participate in SSU meetings at the request of CCB Chairman.
5. The PM DCATS chairs the Engineering Working Group. Composition of the working group will consist primarily of engineers or technical representatives from the following organizations: (1) PM DCATS, (2) WHCA, (3) State Department, (4) DISA, (5) NISO, and (6) 21st Signal Brigade.
6. Funds ISEC support agreement.

Reference: 2009 MOA for SNLC



UNCLASSIFIED FOUO

US Stakeholders Roles and Responsibilities:



USAISEC

1 of 1

1. Provide new UTCP system development (in conjunction with CECOM SEC), testing and fielding
2. Provide new SNLC system development, testing and fielding and fund new SNLC requirements
3. Provide incremental UTCP upgrades as required
4. Provide defective UTCP equipment repair or replacement
5. When applicable, provide equipment disposition
6. Assist MOLINK and State Department in defining new requirements
7. Provide a technical, logistical, and financial feasibility assessment for all new requirements
8. Provide Tier 3 services (SEC will cover software)
9. Collect and review maintenance support needs, make documentation, training or system modifications if necessary
10. Provide initial drawings and documentation as necessary
11. When applicable, provide new equipment training (NET)
12. Assist with hardware configuration management

Reference: 2009 MOA for SNLC



US Stakeholders Roles and Responsibilities:

Software Engineering Center (SEC)

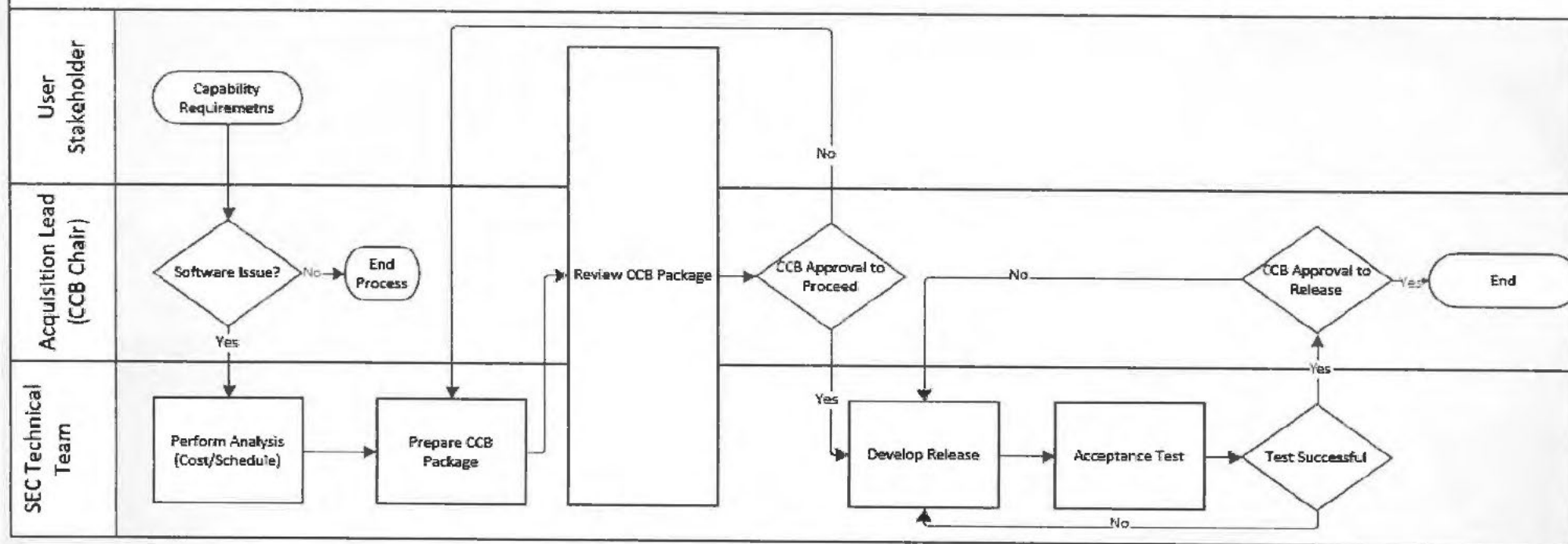
1 of 4

- Provides Post Production Software Support (PPSS)
 - PPSS includes all processes and actions associated with sustaining the software after transition into sustainment
 - PPSS is funded with Operation and Maintenance Army (OMA) funding (1-year funding)
 - SEC is directly funded by DoD Army G4 as part of the annual POM process
- Responsibilities:
 - Infrastructure – maintenance of the software sustainment laboratory (once established through the Transition to Sustainment process)
 - Software Licenses
 - Monthly and Quarterly Cybersecurity updates (addresses security patches and Security Technical Implementation Guide controls)
 - Software Certification and Accreditation including Risk Management Framework and Software Assurance support
 - Code Maintenance/Sustainment – resolve software problems, address software obsolescence
 - Provide technical support

PPSS work flow process



PPSS Workflow Process





US Stakeholders Roles and Responsibilities: Software Engineering Center (SEC)

3 of 4

- If outside of the scope of PPSS, SEC can still provide
 - Software enhancement and sustainment support
 - Certification and Accreditation Support
 - Software Assurance Assessments
 - Field Engineering Support
- Effort must be funded by the organization requesting support through a Functional Support Agreement (FSA)
 - The FSA will identify the scope of work and level of effort
 - Negotiated on an annual basis



US Stakeholders Roles and Responsibilities:

Software Engineering Center (SEC)



4 of 4

1. Provide software configuration management
2. Provide software maintenance (e.g. PPSS) support
3. Assist with the upgrade, testing and fielding of obsolete or existing software systems or capabilities
4. Perform compatibility and regression testing of new crypto equipment software releases if requested by DISA
5. Assist MOLINK in defining new (upgrade) software requirements
6. Assist State Department in defining new (upgrade) requirements
7. Provide Tier 3 software support
8. Provide software documentation as necessary
9. Secure funding for SEC operations
10. Configuration (baseline) control to include documentation for both hardware/software

Reference: 2009 MOA for SNLC



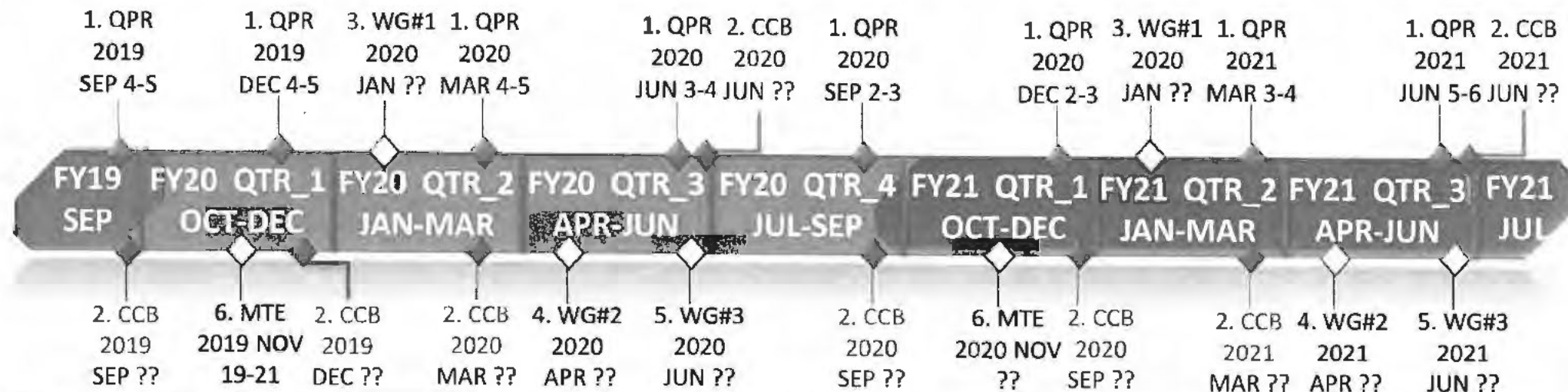
SNLC Battle Rhythm Events

- Validate Battle Rhythm
- Consolidate or combine US meetings as necessary

Battle Rhythm Events						
ID	Event Name	Frequency	Chair/POC	Location	Attendees	Description
1	Quarterly Program Review (QPR)	Quarterly	DISA	FT Meade, MD	US Stakeholders	Synchronization, Accountability, Progress & Program Review
2	Change Configuration Board (CCB)	6 Months	CIO G6	TBD	US Stakeholders	Codified Agreement for Modernization & Tech Refresh
3	Working Group (WG) #1	Annual/JAN	DISA	RU or US	Designated US & RU	Nation-level Wkg Group meetings to control reqts, assign program tasks, develop modernization schedule, discuss status, perform maintenance or testing
4	Working Group (WG) #2	Annual/APR	DISA	RU or US	Designated US & RU	
5	Working Group (WG) #3	Annual/JUN	DISA	RU or US	Designated US & RU	
6	Meeting of Technical Experts (MTE)	Annual/NOV	DISA	RU or US	Designated US & RU	Nation-level discussion on technical improvements and issues
7	US Only Working Group (EWG)	Bi-Weekly	PdM WESS	Phone Conf	WESS, ISEC & SEC	Requirements Receipt, Verification & Validation

US Stakeholders - DISA, MOLINK, WHCA, State Dept, FT Detrick, ISEC, PdM WESS, SEC

Russian Stakeholders - PCD, MOD, MFA, Russia Embassy (DC)



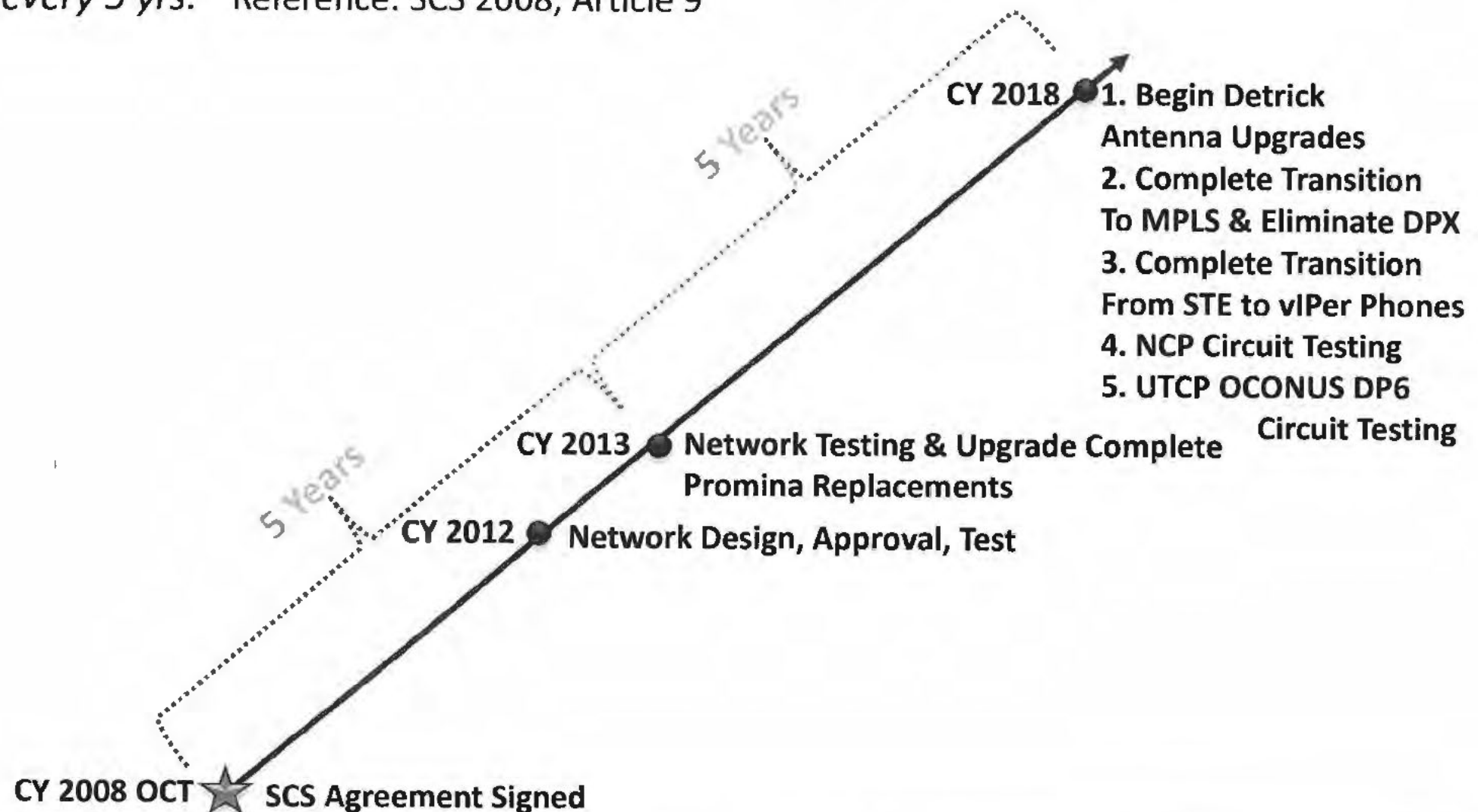


UNCLASSIFIED//FOUO



Modernization Timeline

"Every 2 years the Parties shall develop a program of technical modernization of the Secure Communications System (SCS). The SCS shall be reequipped and updated every 5 yrs." Reference: SCS 2008, Article 9



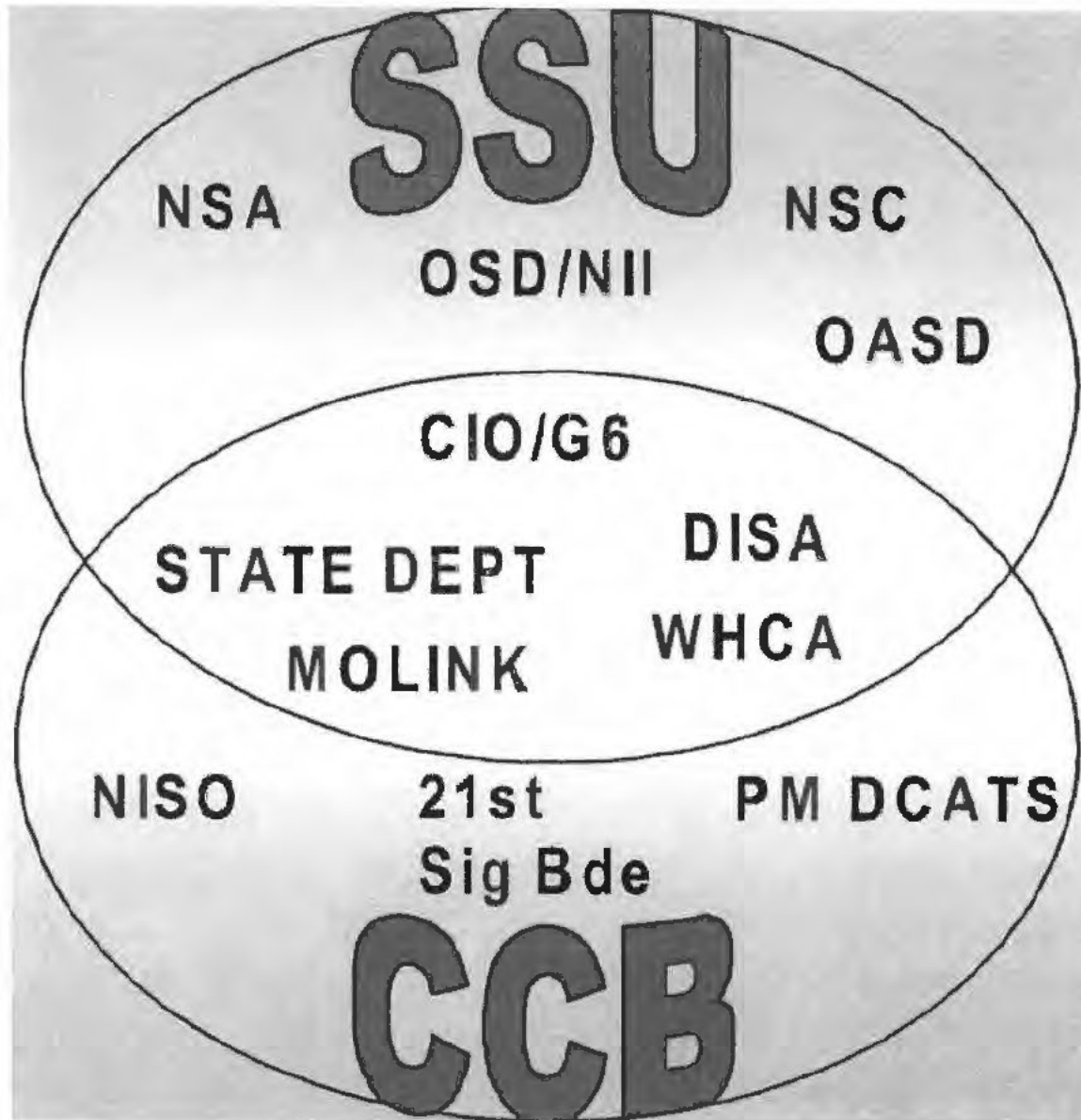
UNCLASSIFIED//FOUO



UNCLASSII //FOUO

Control Configuration Board (CCB)

reference 2012 CCB Charter



1. The Standing Sub-Committee for Upgrades (SSU) is the SECDEF body, authorized by the President, to set technical parameters and establish overall milestone schedules for upgrading the DCL system consistent with U.S./Russian agreements and national Security Policy. The SSU assigns engineering and procurement responsibilities and tracks milestone accomplishments.

2. Army Regulation (AR) 25-1, The Army Information Resources Management Program, directs the CIO/G-6 to provide oversight for National Security Systems (NSS) over Army information systems and other DOD systems for which the Army has been given responsibility, including the DCL program. This CIO/G-6 oversight is exercised thru the CCB.

Figure 1. Relationship and Membership of the SSU and CCB.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Control Configuration Board (CCB)

reference 2012 CCB Charter



Purpose:

- 1) Army methodology to track program status, formulate COAs, & resolve problems.
- 2) Provides direction, tasking, and decisions.
- 3) Determines level of funding required to implement program decisions.
- 4) Ensures coordination with ARSTAFF and Army Secretariat for policy, budgeting, maintenance & modernization.

CCB Members:

- 1) Army Configuration Manager/CCB Chairman
Chief, Land War Net Integration Division/CIO G6
- 2) CCB Secretariat
Civilian Executive Assistant, 21st Signal Brigade
- 3) CCB Member for Systems Acquisition
PM DCATS, PEO EIS
- 4) CCB Member for Network Management
Chief, Direct Communication Links Program Office
Network Infrastructure Services & Opns (NISO)

CCB Advisory Council:

- 1) DISA SNLC Program Manager (Chair)
 - 2) Dept of State
 - 3) Chief of JCS/MOLINK Branch NMCS
 - 4) Commander, WHCA
- The primary responsibility of this group is to provide guidance & assistance to the CCB for integration of policy and directives into system architecture, technical capabilities and sustainment.
 - Provide input to the requirements development & policy for the program.
 - Advise and provide guidance to the CCB on issues the CCB is considering.

UNCLASSIFIED//FOUO



SNLC Network “As-Is”



1. Reconfirm requirements/commitments for each Data Path (i.e. DP 5 test circuit – no commitment to assist in eqpt and funding ie. No requirement for support & DP X) ISEC & PdM WESS
2. Current Trouble Calls/Network Issues (encryption rekey, NRRC outage) ISEC
3. DCL Update (RMF, certification and end user Tests)
Project overview (PdM WESS) & RMF (ISEC)
4. Training (current operator requirements, stakeholder documentation & coordination) – ISEC & PdM WESS – train the trainer
5. Logistics Support (Equipment Inventory, Xfer of Equipment)



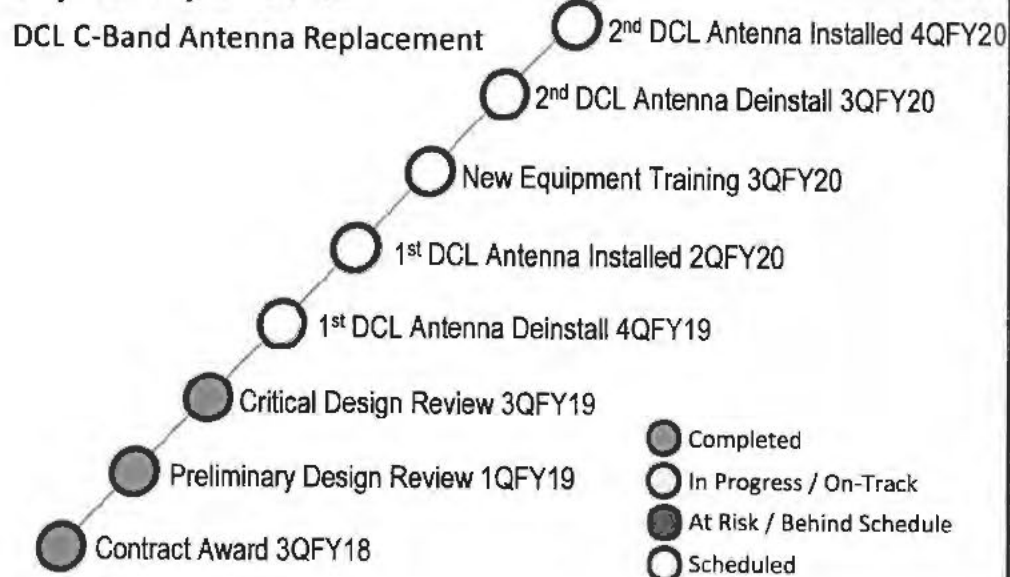
Detrick Earth Station (DES) Direct Communications Link (DCL) Modernization



Project Description

1. De-install Antenna's and platform preparation
2. Platform Load Frames, x2 Antenna's, x2 Shelters, Monitor & Control System (M&C), Interfacility Link (IFL)
3. Test and Integration
4. Provisional Acceptance Certification
5. Training with Training Documentation
6. Technical Manuals
7. Integrated Logistics Support

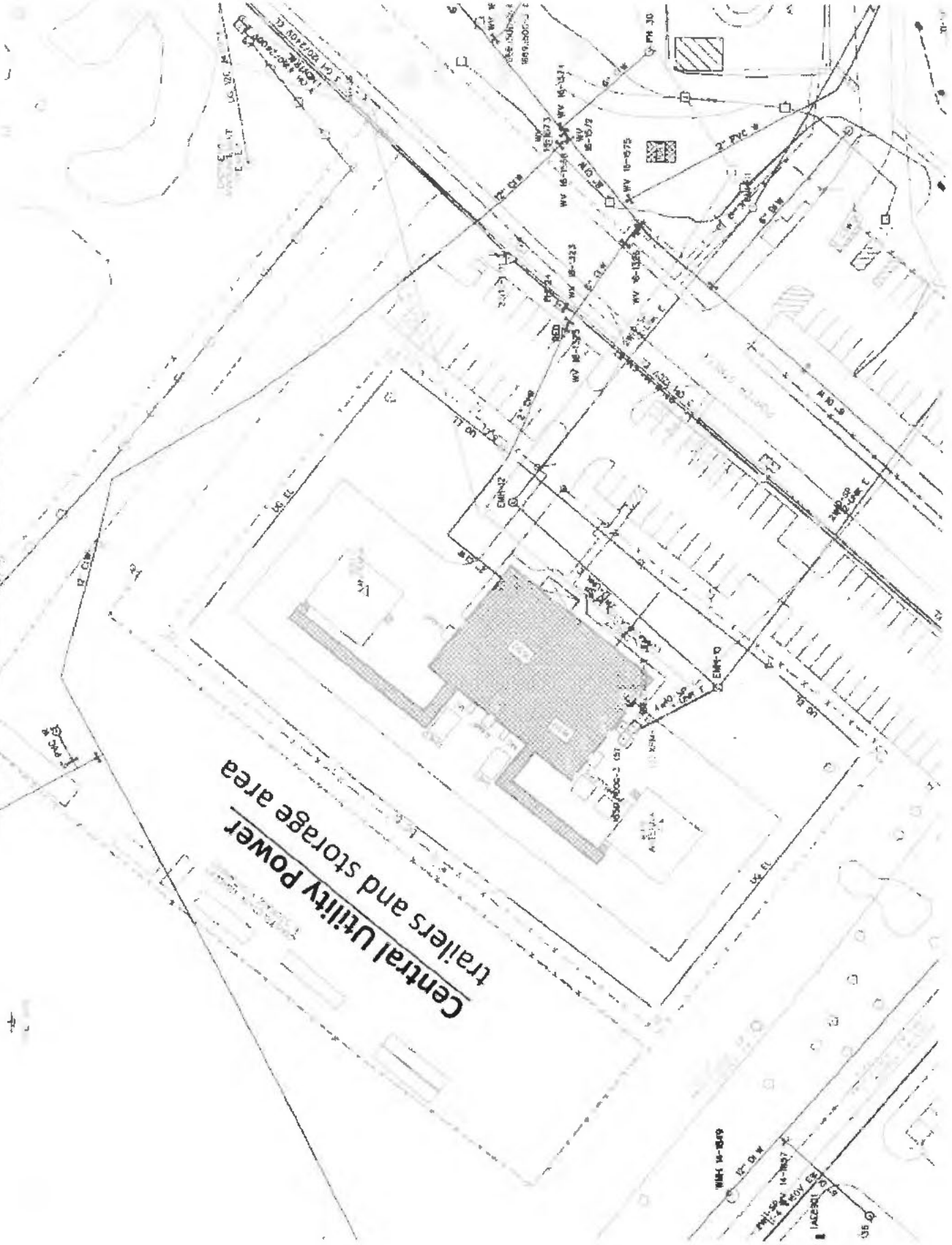
Key Events/Schedule



Discussion Items

- 1) 16 Sep – Antenna B will be deinstalled
 - 2) Schedule Risks:
 - a) Deconflict Road Access with the FT Detrick's Central Utility Power (CUP) Program
 - b) Risk Management Framework (RMF)
- Assessment for RU router and encryption
 - Validation of DAA, requirements and activities

Central Utility Power
trailers and storage area



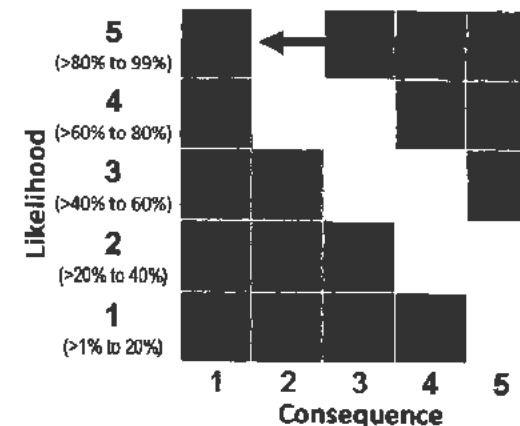


Direct Communications Link (DCL) FT Detrick Central Utility Power Upgrade (CUP)



Risk Statement: IF CUP contractors work activities block access roads 24 Mar – 30 Jun activities THEN this will cause schedule delays that will cause the implementation phase to extend significantly beyond the current Period of Performance (PoP) end dates.

Risk Description: FT Detrick's Central Utility Power (CUP) contractors are scheduled to conduct power work (transformer replacements, power line trenching/maintenance, staging area, heavy vehicle movement, trailer, etc) in the (Detrick Earth Station) DES vicinity 24 Mar 2020 – 30 Jun 2020. With only one main road (Porter St) and minimal access/side roads, the access for heavy vehicles and equipment movement may be impeded for both contractors. Additionally, the DCL contract vehicle and contract period of performance expires on 31 Aug 2020 and the current implementation work activities are scheduled through August; meanwhile, DPWFT Detrick has stated that there contractors and work will cannot be rescheduled based.



Consequence if Realized: Schedule

Risk Handling Strategy: Mitigation

Timeline



Risk Burn-Down Plan

Step	Risk Handling Activity	Status	Owner	S/F Date	LIK	CON
1	SNLC works with ACC-RI to identify alternate courses of action to extend contract's Period of Performance.	In Progress	PdM WESS (SNLC/TYAD)	14 AUG 19 23 MAR 20		
2	SNLC, TYAD and CPI track changes to CUP schedule and scope of work	Not Active	PdM WESS (TYAD/CPI)	14 AUG 19 23 MAR 20		
3	SNLC, TYAD and CPI negotiates and coordinates road usage with DPW, 21 st Sig/302 nd Sig/ASA and CUP contractors during implementation phase	Not Active	PdM WESS (TYAD/CPI)	24 MAR 20 29 JUN 20	5	3



DCL RMF Discussion

Talking points that address three questions

1 of 6

1. Who determines the system Approving Official (AO)
2. Should this system be addressed as a Closed Restricted Network (CRN)(?)
3. Should the system be processed through a customized Risk Management Framework (RMF) process (a customized guide, omitting non-applicable controls?)



DCL RMF Discussion

Identify the Approving Official (AO)

2 of 6

1. DISA, as the system owner, should determine who the System Authorizing Official (AO) should be.
2. This will allow the Security Engineering team obtain the necessary approval for the system's security requirements



DCL RMF Discussion

Is This a Closed Restricted Network?

3 of 6

- The original design the SNLC System was to operate as a closed restricted network (CRN). It should be noted; however, that because the functional architecture of the system includes components that operate within the boundaries of Russia it cannot be ascertained as to whether or not the system operates as a CRN. The United States does not have visibility of any components on the far side therefore cannot state there are no other connections to the SNLC System.
- Russia, a non-NATO partner is not accountable to United States laws or regulations, therefore there is no way an inspection can be performed of the complete system for compliance. Because of these inherent challenges, the inherited risk of this system will always be categorized as HIGH.



DCL RMF Discussion SNLC System RMF 4 of 6

Discussions with the US ARMYISEC SCA-V it was determined that:

- The SNLC, UTCP, DCL should be combined into one accreditation boundary (example SNLC System)
- Combined system would then go through a modified RMF process
- Because of the nuances of these systems, it would be best to not register the system in eMASS.
- Registering this very sensitive system, to include all of the insecure settings as well as risks into the eMASS system would allow others visibility which may not be appropriate



DCL RMF Discussion

SNLC System RMF

5 of 6

- The RMF process will be used as a security engineering guide to specifically address the Integrity and Availability controls required for the system.
- Fundamentally the risk will be categorized as **High** for most of the identified controls because of the deployed environment as well as the overall mission of the system.
- A RMF package which includes all insecurities and risks associated with this system should be created outside of the eMASS.
- This package would be submitted to the AO that outlines operating the system in the configuration necessary for the mission, allowing the AO to accept the risk.



DCL RMF Discussion

Items Necessary for RMF Evaluation:

6 of 6

- Baseline system
- Evaluation of system to include scans, configuration settings, etc
- Processes for lifecycle management (configuration management, account management, etc)
- Required RMF overlays would have to be created – as necessary
- Security Engineering Assessment Report (RMF package) and POAM would have to be created and then submitted to the AO for review and approval to operate



Training Case Study/AAR: Management Server 1 of 5

The 2018 Management Server training covered the following topics:

- **RADIUS Services**
- **Solarwinds Network Performance Monitor (NPM)**
- **Vine Encryption Device Management and Monitoring**

This training was provided by ISEC to MOLINK personnel



Training Case Study/AAR: Management Server 2 of 5

Steps to take before the next training is scheduled:

Solicit end users for information that includes:

- Who needs to be trained,
- Identify who needs basic user training, who needs administrative user training.
- Specifically what they feel needs to be covered in this training



Training Case Study/AAR: Management Server 3 of 5

Future training should be more user specific
To include:

- Deeper coverage into Alerts and reporting capabilities of NPM
- Emphasis on “Train the Trainer” for both Administrative and User functions of these servers
- Provide instruction rosters that provide Training dates, content, and participation information



Training Case Study/AAR: Management Server 4 of 5

Other training should also include

- UTCP server operations and troubleshooting
- Emphasis on “Train the Trainer” the UTCP
- Provide instruction rosters that provide Training dates, content, and participation information



Training Case Study/AAR: Management Server 5 of 5

Additional notes for the management servers

- 1. Training should also include notifying users that the servers are live and should be monitored.
- 2. We need to change the user home screen so that alerts are visible at a glance
- 3. Propose a very large screen (wall mount) so that all four of the servers (management and Vine servers) can be visible on a single screen with 4 simultaneous views



U.S. ARMY

UNCLASSIFIED//FOUO



Acronym	Definition
ARUK	American, Russia, UK
CL	Communication Lines
DCL	Data Communications Link
DCL	Data Crisis Link
DISA	Defense Information Systems Agency
DoS	Department of State
DP	Data Path
DVL	Direct Voice Link
GTC	Gateway Telecommunications Center
HoS	Heads of State
ICT	Intermediate Control Terminal
IM	Information Management
ITMC	International Technical Maintenance Center
ITU	International Telecommunication Union
JS	Joint Staff
MOD	Ministry of Defense (Russia)
MOLINK	Washington-Moscow Hotline
MPP	Modernization Program Plan
NP	National Path
NSA	National Security Advisor
NSC	National Security Council
PCD	Presidential Communications Directorate (Russia)
PM	Program Manager
RSSC	Russian State Satellite Company
SCS	Secure Communication Systems
SSOG	Satellite Systems Operating Guide
STE	Secure Telecommunications Equipment
TC	Telecommunications Channel
TMDE	Test, Measurement, Diagnostic Equipment
VP	Vice President
WG	Working Group
WHCA	White House Communications Agency



Schedule

Date	Time	Event	Location	References
Wednesday, September 4, 2019	1000 - 1100	Stakeholders Roles & Responsibilities	TBD FT Detrick, MD	SNLC Charter, MOA 2009
Wednesday, September 4, 2019	1100 - 1200	Battle Rythm Events	TBD FT Detrick, MD	SNLC Charter, MOA 2009
Wednesday, September 4, 2019	1200 - 1300	Lunch	FT Detrick, MD	NA
Wednesday, September 4, 2019	1300 - 1600	SNLC Current Network	TBD FT Detrick, MD	SNLC Network Baseline
Thursday, September 5, 2019	1000 - 1600	SNLC Network "To-Be	TBD FT Detrick, MD	SNLC Charter, MOA 2009

Administrative Coordination:

1) Please send VAR to both Security offices.

21st SMO Code WDSXAA

302nd SMO Code WHBWAA

POC: Mr. [REDACTED] [REDACTED]@mail.mil,

Desk 301-619-3601, Cell [REDACTED]

2) Pickup badges from 302nd Bn S2 office

1671 Nelson St.

Ft Detrick, MD

3) QPR will be in Bldg 1668, Unclassified Conference Room



UNCLASSIFIED//FOUO

Agenda from Quarterly Program Review Apr 2019



ISEC Apr 2019
Trip Report

1. Current status of network
2. Remaining tasks to accomplish to bring the system online
3. Status of MET upgrade, including timeline
4. Upgraded network (gig-ether vice T1s, particularly on the U.S. Terrestrial)
5. OTAT of key across the network
6. 23-25 April PCD Working group in DC
7. Status of NRRC transition
8. What we need to do to move the DTL to the new network
9. What we need to do to move the CJCS VTC to a different path
10. Renew COMSEC Hand Receipt for the 250Xs
11. Budget issues



Due Outs from 9-11 April 2019 QPR

1. DISA will contact the Russian side to facilitate direct communications with the Russian satellite communications provider in order to determine if there are connectivity/certification requirements for the earth station to connect to the AM-44 satellite, similar to the requirements in place with Intelsat. This is in conjunction with the deployment of the MET upgrade
2. DCL Authority to Transmit (ATT) and Authority to Operate (ATO) Form 312. Is DISA the certifying official?
3. Revisit Memorandum of Agreement (MOA) from 2009 to validate US current stakeholder roles and responsibilities
4. DISA Modernization Efforts Timeline –
 - a) transition to a full Ethernet network, rather than the T1 network being deployed;
 - b) update and modernization of cryptographic hardware;
 - c) replacement of cryptographic hardware at the ISEC R&D facility;
 - d) network updates; server virtualization; and geographic diversification of the supporting network elements
 - e) SEC Initiatives - CHAT system, trouble ticket system, review operating systems for the DCL UTCP (User Terminal Communications Platform) terminals as well as management of licenses for deployed/deploying software suites, offline message processing terminals



CIO G6 CCB Discussion

1. 2008 Secure Communications System Agreement. (PdM WESS) Agreement between the United States and the Russian Federation, the communications equipment supporting the DCL and other executive-level communications capabilities is to be regularly reviewed and modernized.

2. Draft NSPM (National Security). (DISA, CIO G6, PdM WESS/ISEC)

3. Change Configuration Board. (CIO G6)



T1 Request to DISA 24 July

TIMELINE:

- Will our team receive a plan of action and milestone for related systems? This plan of action and milestones document/information will allow for us to plan and provide access for certain spaces for the install/configurations.
- What's the timeline for conducting a full system online verification test (SOVT)?
- Is there an tentative date for bringing systems online?

TRAINING:

- How will training and documentation be delivered to my team?
- When would we receive these items in accordance with the plan for completion of discussed system?

SITE LOCATION INSTALL:

- Who's removing and taking the old gear and parts for all locations? I need to make arrangements for space access so personnel will be allowed to carry such items.

SYSTEM CHANGES:

- From the working group I learned that DP-X will no longer be utilized. Is there a reason for this, and why is this the case?
- Does the communication circuit maintain HEMP protections?

DEFINITION OF COMPLETION:

- It was stated that once we're able to send a message to the distant end then our system would then be considered online and operational. This is unfortunately is not true, we still have to bring online related systems to test and verify they work as well.
- From recent working group it's unclear what completion of modernization for this circuit looks like. Can someone elaborate or explain the steps and actions to completion?



UNCLASSIFIED//FOUO

Dueouts

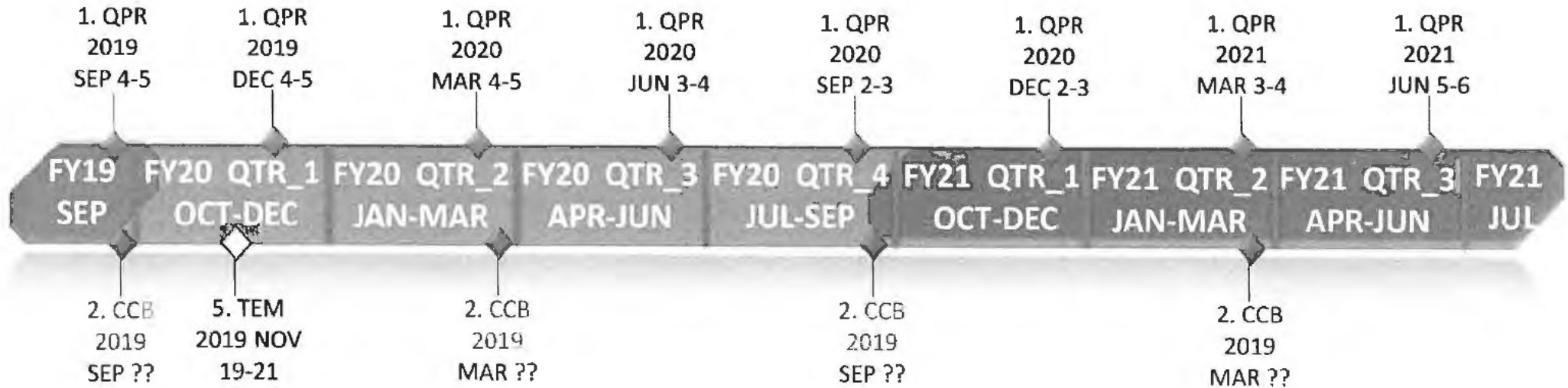




UNCLASSIFIED//FOUO



SNLC Battle Rhythm Events



Battle Rhythm Events		
ID	Event Name	Frequency
1	Quarterly Program Review (QPR)	Quarterly
2	Change Configuration Board (CCB)	6 Months
3	Engineering Working Group (EWG) #1	APR
4	Engineering Working Group (EWG) #2	JUN
5	Technical Experts Meeting (TEM)	NOV
6	PdM WESS, ISEC & SEC	Monthly



UNCLASSIFIED//FOUO