BY ORDER OF THE COMMANDER
JOINT BASE ELMENDORF-RICHARDSON

JOINT BASE ELMENDORF-RICHARDSON INSTRUCTION 17-130

19 OCTOBER 2022

Cyberspace

NETWORK SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This Publication is available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading and ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 673CS/CYNC

Certified by: 673CS/CC
(Lt Col Charles A. Barton III)

Supersedes: JBELMENDORF-RICHARDSONI17-130, 11 October 2018

Pages: 13

This publication implements Air Force Instruction (AFI) 17-130, *Cybersecurity Program Management.* This instruction establishes guidance concerning network security accountability on all networks and information systems provided by the 673d Air Base Wing (673 ABW). It applies to all users of Joint Base Elmendorf-Richardson (JBER) Air Force Networks (AFNet), both Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet) to include Air National Guard and Air Force Reserve personnel. Failure to observe the prohibitions and mandatory provisions in **paragraph 8.6.4** of this publication by military members constitutes a violation of Article 92(1) of the Uniform Code of Military Justice (UCMJ). Article 92(1) of the UCMJ does not apply to members of the ANG while in Title 32 status (that is, activated for state duty under state command), but ANG members may be subject to an equivalent article under a state military justice code. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a tier number (T-0, T-1, T-2, or T-3) following the compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*, (Attachment 10) for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority or to the publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial

product, commodity, or service in this publication does not imply endorsement by the Air Force (AF). Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include updated references, formatting, and clarification of processes.

1. Overview. The purpose of this Network Security Instruction is to outline the responsibilities of every user operating on JBER's AFNet. This publication defines a network security incident as any activity, event, or action that violates policy, guidance, or directives; introduces additional vulnerabilities; or increases risk to the network or 673 ABW information systems.

2. Roles and Responsibilities. All personnel utilizing JBER's NIPR and/or SIPR networks must comply with all policies and guidance included in this instruction. Failure to comply will result in users, devices, files, etc. being removed from AFNet.

2.1. 673d Air Base Wing Commander (673 ABW/CC): has the overall responsibility of implementing the Cybersecurity program for JBER's NIPR and SIPR information systems and ensures users comply with AFI 17-130, *Cybersecurity Program Management*.

2.2. 673d Communications Squadron Commander (673 CS/CC):

2.2.1. Is the lead for all cybersecurity and Computer Security (COMPUSEC) accounting for JBER's NIPR and SIPR networks.

2.2.2. Is responsible for initiating actions to improve or restore the cybersecurity posture of the networks, optimizing network rules and procedures that balance mission assurance and risk mitigation.

2.2.3. Will perform an annual review of all cybersecurity programs that fall under the 673 ABW.

2.3. Wing Cybersecurity Office (WCO).

2.3.1. The WCO provides cybersecurity program assistance and guidance to the host wing for COMPUSEC, Risk Management Framework, vulnerability hunt, remanence security, privileged user access, data loss prevention, and TEMPEST requirements.

2.3.2. The WCO ensures unit Cybersecurity Liaisons (CLs) are informed on AF policies for all networks and information systems that fall under 673 ABW purview.

2.4. Wing Knowledge Management Center: provides direct support to JBER personnel in areas of Enterprise Information Services (i.e., SharePoint®), Privacy Act, JBER Publications and Forms and Electronic Records Management (i.e., Official Records) responsibilities. **Note:** The 673d Communications Squadron Knowledge Management Center (CS/CYNK) is the Wing Knowledge Management Center.

2.5. JBER CLs:

2.5.1. Act as the single liaison between their unit and the Information System Security Manager for all COMPUSEC matters to include the Information Assurance Awareness and Notice and Consent programs.

2.5.2. Will provide oversight to ensure that all Department of Defense (DOD), AF, and local policies and procedures are used according to current publications.

2.5.3. Ensure all users meet the pre-requisites and are aware of their responsibilities before being granted access to AF information systems IAW DAFMAN 17-1304, *Identity, Credential and Access Management (ICAM),* paragraph 5.4.

2.5.4. CLs must be appointed in writing by their unit commander and attend all training sessions as mandated.

2.6. Privileged Users. Privileged users are any Information Technology (IT) technician with specialized training and granted administrative rights IAW DAFMAN 17-1304, paragraph 5.4.3., to perform unique mission requirements on JBER's NIPR and/or SIPR networks.

2.6.1. Privileged users include: Functional System Administrators (FSA), Client Support Administrators (CSA), Client System Technicians (CST), and Program Management Office (PMO) system administrators.

3. Clearance, Training, and User Agreements.

3.1. Clearance. Users and system support personnel must have the required security clearance, authorization, and need to know before being granted access to any 673 ABW network or information systems.

3.2. Training. Trained and knowledgeable information resource users and administrators are a key element of defense-in-depth. A viable cybersecurity program must include initial, periodic, supplemental, and remedial training to develop and maintain knowledgeable information resource users and administrators.

3.3. User Agreement. User agreements (AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision*) are mandatory IAW DAFMAN 17-1301, *Computer Security (COMPUSEC),* and must be completed prior to gaining access to JBER's NIPR and SIPR information systems and networks. User agreements are provided by unit CLs.

4. Negligent Discharge of Classified Information (NDCI): is a security incident resulting in the unauthorized transfer of information on a system, application, or media below the classification of the information. All AFNet users are responsible for the protection of sensitive and classified information. If a potential classified material incident has been detected on any electronic media, take the following actions:

4.1. Incident Reporting. Personnel should refer to the JBER Incident Reporting Aid upon the detection of a potential NDCI. IAW TASKORD 2019-007-001A, *Negligent Discharge of Classified Information (NDCI) Handling Procedures.*

4.1.1. All personnel who become aware of a possible NDCI shall immediately report it to their area security manager, supervisor, commander, or director.

4.1.1.1. Supervisors and area security managers will report the security incident to their commander or director.

4.1.1.2. Commanders, directors, and/or security managers will work with the Wing Information Protection Office (WIPO) to determine if the incident meets the NDCI criteria.

4.1.1.2.1. If it is determined that an NDCI occurred, the offending unit's commander will request an official NDCI declaration letter from their respective group commander, wing commander, or the 673 CS/CC.

4.1.1.2.2. The declaring group commander, wing commander, or 673 CS/CC will send the signed declaration letter to the Communications Focal Point (CFP) for transmission to the 690th Network Support Squadron (NSS).

4.1.1.2.2.1. The 690 NSS will coordinate and track all NDCI events.

4.1.1.2.2.2. The CFP will coordinate and direct all local sanitization efforts.

4.1.2. Personnel will comply with the "JBER Incident Reporting Aid". The JBER Incident Reporting Aid can be downloaded from the WCO SharePoint® site located at: **https://usaf.dps.mil/sites/jber/673ABW/673MSG/CSMPNP/SCX/SCXS/SitePages/Home.aspx**.

4.2. The CFP and the WCO will support and guide affected unit commanders, security managers, and CL's as they navigate the NDCI process

4.3. The offending user(s) will be required to complete the process outlined in TASKORD 2019-007-001A, section 6, prior to having their account unlocked.

4.4. User accounts locked due to receiving an NDCI message will be enabled after enterprise sanitization is complete.

4.5. The 690 NSS will direct the CFP to return computers, and mobile devices after sanitization has been completed.

5. Virus/Malicious Software Reporting: AFNet users shall refer to the JBER Incident Reporting Aid upon detection of a potential virus or malicious software.

5.1. Disconnect the network cable, leave the system powered on, and immediately contact your CL and the CFP at 552-2666 option #3. The machine will not be used until further guidance is received from the CFP.

5.2. Annotate any prompts or messages on the monitor and provide the information to your CL.

5.3. The 673 Communications Squadron (673 CS) will conduct a full virus scan of the machine and determine if the virus scan cleaned the machine.

6. Network Vulnerability Management Policy.

6.1. Maintain Secure Baseline. IAW TO 00-33A-1109, *Methods and Procedures—Air Force Information Network (AFIN) Vulnerability Management*, all systems (desktops, laptops, notebooks, servers) on both NIPR and SIPR network enclaves must meet minimum Defense Information Systems Agency Security Technical Implementation Guides (STIG) and Air Forces Cyber (AFCYBER) baseline security patch/update requirements.

6.1.1. Systems that fail to meet the secure baseline standards will be identified as non-compliant and will be blocked and/or removed from the network.

6.1.2. Remediation for Non-Compliant Systems. When a customer's system is blocked or removed from the network, actions required to restore access will be determined by Enclave and PMO status

6.1.2.1. For NIPR Enclave: Contact your CL or call 552-2666 option 1 for assistance. Responsibility for patching, applying STIG configuration, and remediating NIPR legacy non-PMO systems belong to Enterprise Information Technology as a Service (EITaaS) partners per 616 OC TASKORD, *Subject: EITAAS Risk Reduction Effort (RRE) Roles and Responsibilities*.

6.1.2.1.1. EITaaS partners will have two weeks to patch, remediate, and coordinate a rescan with 673 CS Vulnerability Management

6.1.2.1.2. Enterprise Desktop Configuration (EDC) Systems. EDC systems are managed by EITaaS partners. EDC systems are subject to EITaaS partners' own vulnerability management and remediation plan and procedure that must be reported to the local 673 CS leadership for visibility.

6.1.2.2. For SIPR Enclave: Contact your CL or call 552-2666, option 1, for assistance.

6.1.2.2.1. Responsibility for patching, applying STIG configuration, and remediating legacy systems belong to 673 CS CST or Unit CST, FSA, or CSA that owns the identified non-compliant system.

6.1.2.2.2. 673 CS CST or Unit CST, FSA, or CSA will have two weeks to patch, remediate, and coordinate rescan with 673 CS Vulnerability Hunt.

6.1.2.3. Program Management Office (PMO) Systems. PMO system administrators will be provided Assured Compliance Assessment Solution (ACAS) results of the systems they manage

6.1.2.3.1. PMO administrators will apply applicable patches and updates to their system as allowed by their PMO.

6.1.2.3.1.1. For every patch and update that cannot be applied per the PMO, or if ACAS results on their system(s) show a Weighted Vulnerability Index (WVI) of 5.0 or greater, or the system(s) has/have failed credentialed access, the PMO administrator must provide a Plan of Action and Milestones.

6.1.2.3.1.2. The PMO system(s) is/are subjected to the local quarantine policy and TO 00-33A-1109 for failure to comply with the listed requirements.

6.2. Network Uptime Requirements. All network devices (desktop, laptops, switches, printers, etc.) on NIPRNet and SIPRNet must be powered on and connected to the network to ensure an up-to-date secure baseline.

6.2.1. SIPRNet Uptime**.** SIPRNet devices, to include thick client systems (desktop and laptop devices), and High Assurance Internet Protocol Encryptors to include TACLANEs, must be powered on and connected to the network, at a minimum, every Wednesday from 0900 to 1500 Alaska Standard Time (AKST). This is when 673 CS executes network scans for United States Cyber Command (USCYBERCOM) requirements and applies necessary security updates to be downloaded.

6.2.1.1. Systems failing to connect during the uptime window will be identified as non-compliant.

6.2.1.2. Systems identified as non-compliant will be removed or blocked from the network.

6.3. System Restart Policy. Users must restart their workstation once a week, at a minimum, to ensure that updates have completely installed.

7. User Account Management.

7.1. Account Inactivity. Inactive user accounts create security and management concerns and will be removed from the network in accordance with DAFMAN 17-1301. When a user does not log into a networked device on JBER for an extended period, the user's account is flagged inactive and will be deleted as outlined below.

7.1.1. SIPRNet exercise participant accounts provisioned on the JBER network will be deleted 15 days after temporary duty (TDY) conclusion. Visiting members must notify the CFP at 552-2666 option 3 for departure delays and if an extension of account access is required beyond the planned exercise window.

7.1.2. Inactive NIPR/SIPRNet accounts will be disabled after 30 days.

7.1.3. Inactive NIPR/SIPRNet accounts will be deactivated after 90 days.

7.1.4. For users that are frequently TDY or travel through JBER and need an exemption from this policy, contact the CFP 552-2666 option 3 for guidance.

8. Electronically Stored Information.

8.1. Common Shared Drives. JBER shared drives can be used by personnel to store data considered to be Controlled Unclassified Information (CUI). For access or permissions to shared drives, contact your unit CL.

8.1.1. Personally Identifiable Information (PII) stored on the shared drives, along with subfolders and directories, need be locked and must comply with AFI 33-332, *Air Force Privacy and Civil Liberties Program.* This will ensure PII is accessible only to individuals whose official duties provide them a valid need-to-know, security measures or encryption is applied, and proper labeling of the file is achieved.

8.2. Official Records. Official electronic records must be stored on the Electronic Records Management Drive (\\ELFS1). This drive will be used only to manage official records IAW AFI 33-322, *Records Management Program*, and the JBER Records Management Plan.

8.3. SharePoint®. All PII on SharePoint® must be controlled by group permissions and comply with AFI 33-332, allowing access only to individuals whose official duties provide them a valid need-to-know. Unit Privacy Monitors and Content Managers are required to conduct monthly scans of their unit's SharePoint® sites. If unprotected PII data is discovered during the scan, delete and/or safeguard PII and submit a collective PII breach report (DoD Form 2959) to the base Privacy Manager.

8.4. Access Requests. Users requesting access to shared drives or Official Records/Electronic Records Management drives must contact their unit CL to validate their need-to-know and to request appropriate permissions for access via Information Assurance Officer Express.

8.5. Safeguarding PII. PII must be accessible only to individuals who have an official need-to-know IAW AFI 33-332. Additionally, all folders that contain PII must be labeled "CUI" or "PII".

8.6. Compliance Enforcement. Personal Storage Tables (PSTs), user profiles, personal folders and non-mission related personal data will not be permitted on the shared drives as they are presumed to contain unencrypted CUI and PII. PSTs are not considered official records.

8.6.1. 673 CS will scan shared drives and official electronic records weekly for unauthorized PSTs, user profiles, non-mission related personal files and data.

8.6.1.1. Examples of personal data includes but is not limited to: documents relating to off duty education, W-2's, out/in-processing, marriage licenses, divorce decrees, commissioning packages, medical/dental, mortgage/housing, vehicle registration, records from Personnel Records Display Application, and retirement/separation. **Note:** Personal data can be stored in Microsoft OneDrive®.

8.6.1.2. Unauthorized files on shared drives will be deleted without notice to the owner.

8.6.1.3. Repeated violations will result in the loss of the user's network access and notification to their chain of command.

8.6.2. Unit Privacy Monitors must conduct semi-annual reports as directed by the wing privacy manager IAW AFI 33-332. Semi-annual reports will consist of the number of records reviewed, privacy complaints, and training provided.

8.6.3. Unit Content Managers must conduct semi-annual reviews of their SharePoint® sites to ensure PII is either removed or protected via SharePoint® group permissions IAW AFI 33-332. **Note:** Commanders must identify Unit Content Manager(s) via email to the JBER EIS Inbox at: **3cs.x.1@us.af.mil**.

8.6.4. All unprotected PII files discovered on SharePoint® or JBER shared drives will be deleted and/or safeguarded and a collective PII breach report (Department of Defense Form 2959) will be submitted. Potential or actual breaches must be reported to the servicing Privacy Manager/Monitor by anyone discovering it. Failure by military members to obey the mandatory provision of this paragraph is a violation of Title 10 US Code Chapter 47 Section 892 UCMJ Article 92(1), *Failure to Obey Order or Regulation*. Civilians who violate information security policy may be disciplined in accordance with Department of the Air Force Instruction (DAFI) 36-148, *Discipline and Adverse Actions of Civilian Employees.*

8.7. **PII Breach Reporting.**

8.7.1. Once personnel become aware of PII loss, theft, or compromise, whether electronic, paper, or verbal it must be immediately reported. Report the breach to your supervisor, unit Privacy Monitor, and the JBER Privacy Officer at 551-7109 or email at **JBER.FOIA@us.af.mil**.

8.7.2. The JBER Privacy Officer will assist the unit monitor with conducting a risk assessment and submitting a mandatory PII Breach Report for the individuals involved or affected by the breach.

9. Removable Media.

9.1. Non-Approved Flash Media Devices. The use of flash media on DOD networks is prohibited per USCYBERCOM Communications Tasking Order (CTO) 10-084.

9.1.1. Only mission critical devices listed on a unit's whitelist waiver are authorized for use on the network. **Note:** Solid State Drives are not authorized.

9.1.2. Unit CLs will maintain a master whitelist of authorized devices. Users should contact their CLs for guidance.

9.1.3. The Unit Commander and the first O-6 in the Chain of Command must both approve and sign the whitelist waiver prior to submitting to the WCO for approval.

9.2. **Approved Flash Media.** Flash media devices that are authorized on the network, via whitelist, must meet the following criteria:

9.2.1. Devices must be government purchased and added to the unit accountable property officer's IT Asset Management account.

9.2.2. External hard drives must be virus scanned and encrypted with Encryption Wizard or BitLocker® (users are responsible for BitLocker® passwords and maintaining recovery keys). **Note:** The 673 CS does not have the ability to restore BitLocker® passwords.

9.2.3. External drives must be formatted with New Technology File System (NTFS) with default software removed.

9.3. Portable Electronic Devices (PEDs) in Classified Processing/Secure Open Storage Areas

9.3.1. The introduction of any PEDs into any JBER classified meeting, processing, or Secure Open Storage area is prohibited. PEDs are devices capable of sending, receiving, monitoring, recording, or processing voice or signals, image capturing, and utilizing wireless (Bluetooth®, Infra-Red, and Radio Frequency) transmission of information. Personal wearable activity monitors, fitness, multisport, Global Positioning System, and any wireless headphones are PEDs.

9.3.2. Wireless capabilities being permitted in areas where classified information is discussed or processed first requires written approval from the AF Enterprise Authorizing Official and the AF Certified TEMPEST Technical Authority according to Department of Defense Directive (DoDD) 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*. The WCO can guide Unit CLs through this process and can be reached at 552-9426.

9.4. Personally Owned Flash Media Devices include: external hard disk drives, phones, cameras, fitness devices, etc., are prohibited for use on the JBER network.

9.5. Universal Serial Bus (USB) Violations. Connection of personally owned flash devices or flash devices not identified via whitelist waivers is a violation of AF Designated Authorizing Authority Combined Implementation Guidance for the USCYBERCOM CTOs 10-084 and 10-133 and will result in a USB violation.

9.5.1. Consequences for violating CTO 10-084 are as follows:

9.5.1.1. Users will lose network privileges until the investigation is complete.

9.5.1.2. Users must re-accomplish DoD Cyber Awareness Challenge and DoD Mobile Devices training and provide completion certificates to the WCO. The required training is located at: **https://cyber.mil/training/cyber-awareness-challenge/** and is available from any public or home computer.

9.5.1.3. The violating member's Squadron Commander will direct the unit CL to perform an investigation, will sign the final report, and forward to the WCO.

9.5.1.4. The workstation will be re-imaged before re-use.

9.5.1.5. The JBER Information System Security Manager will review the report and certificates and make a recommendation on account re-instatement to the 673 CS/CC.

9.5.1.5.1. The 673 CS/CC is the authority for re-instatement of network privileges. If the user's access to the network is mission critical, the first O-6 in the member's chain of command must contact the 673d Mission Support Group Commander (673 MSG/CC) to request remediation.

10. Administrative Accounts. Administrative accounts will be granted to privileged users that have unique mission requirements IAW DAFMAN 17-1304, paragraphs 5.4.3. and 5.5.9.

10.1. Privileged users must meet DoD 8570.01-M, *Information Assurance Workforce Improvement Program,* and Air Force Manual (AFMAN) 17-1303, *Air Force Cybersecurity Workforce Improvement Program,* requirements.

10.2. All privileged user requirements are listed on the JBER WCO SharePoint® site: **https://usaf.dps.mil/sites/jber/673ABW/673MSG/CSMPNP/SCX/SCXS/SitePages/Home.aspx**.

DAVID J. WILSON, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 USC Chapter 47 §892 UCMJ Art. 92(1), *Failure to Obey Order or Regulation*

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, 14 April 2004

DAFI 36-148, *Discipline and Adverse Actions of Civilian Employees*, 27 September 2022

DAFMAN 17-1301, *Computer Security (COMPUSEC)*, 12 February 2020

DAFMAN 17-1304, *Identity, Credential and Access Management (ICAM)*, 18 August 2021

DAFMAN 90-161, *Publishing Processes and Procedures*, 15 April 2022

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFMAN 17-1303, *Air Force Cybersecurity Workforce Improvement Program*, 12 May 2020

TASKORD 2019-007-001A, Subject: *Negligent Discharge of Classified Information (NDCI) Handling Procedures*

616 OC TASKORD, Subject: *EITAAS Risk Reduction Effort (RRE) Roles and Responsibilities*

TO 00-33A-1109, *Methods and Procedures—Air Force Information Network (AFIN) Vulnerability Management*

USCYBERCOM CTO 10-084

USCYBERCOM CTO 10-133

Joint Base Elmendorf-Richardson Memorandum, *Records Management Plan*, March 2022

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision*

Abbreviations and Acronyms

ACAS—Assured Compliance Assessment Solution

AF—Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAN—Air Force Manual

AFNET—Air Force Network

CL—Cybersecurity Liaison

COMPUSEC—Computer Security

CFP—Communications Focal Point

CSA—Client Support Administration

CST—Client System Technician

CTO—Communications Tasking Order

CUI—Controlled Unclassified Information

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DoD—Department of Defense

DoDD—Department of Defense Directive

EDC—Enterprise Desktop Configuration

EITaaS—Enterprise Information Technology as a Service

FSA—Functional System Administration

IAW—In Accordance With

IT—Information Technology

JBER—Joint Base Elmendorf-Richardson

NDCI—Negligent Discharge of Classified Information

NIPRNet—Non-Secure Internet Protocol Router Network

NTFS—New Technology File System

OPR—Office of Primary Responsibility

PED—Portable Electronic Device

PII—Personally Identifiable Information

PMO—Program Management Office

PST—Personal Storage Table

SIPRNet—Secure Internet Protocol Router Network

STIG—Security Technical Implementation Guides

TDY—Temporary Duty

TO—Technical Order

UCMJ—Uniform Code of Military Justice

USB—Universal Serial Bus

USCYBERCOM—United States Cyber Command

WCO—Wing Cybersecurity Office (also known as CS/CYNC)

WIPO—Wing Information Protection Office

WVI—Weighted Vulnerability Index

Office Symbols

ABW—Air Base Wing

ABW/CC—Air Base Wing Commander

CS—Communications Squadron

CS/CC—Communications Squadron Commander

CS/CYNC—Communications Squadron Cybersecurity (referred to as WCO)

CS/CYNK—Communications Squadron Knowledge Management

MSG/CC—Mission Support Group Commander

NSS—Network Support Squadron