BY ORDER OF THE COMMANDER
35TH FIGHTER WING

35TH FIGHTER WING INSTRUCTION
17-103

13 JANUARY 2017
Certified Current on 17 October 2024
Cyberspace

COMMUNICATIONS
SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 35 CS/SCXS

Certified by: 35 CS/CC
(Lt Col Angelique Nelson)

Supersedes: 35FWI33-103, 15 April 2015

Pages: 37

This fighter wing instruction implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, as well as Methods and Procedures Technical Order (MPTO) 00-33A-1109, *Air Force Information Network (AFIN) Vulnerability Management*, and contains local guidelines and procedures for managing Air Force Telephone Systems at Misawa Air Base.

Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Additionally, if the publication generates a report(s), alert readers in a statement and cite all applicable Reports Control Numbers in accordance with Air Force Instruction (AFI) 33-324. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Form 847s from the field through the appropriate functional's chain of command.

SUMMARY OF CHANGES

Replaces any previous editions of 35th Fighter Wing Instruction (FWI) 33-103. Changes include: Work Order Management System (WOMS) ticket expiration details; Wing Cyber Readiness Program (CRP) roles, responsibilities, and procedures; definition of new responsibilities for Cybersecurity Liaisons (CLs) vs Telephone Control Officers (TCOs);

replacing the Telecommunications Monitoring and Assessment Program (TMAP) with Cyberspace Defense Analysis (CDA); definition of unit Resource Advisors (RA) responsibilities; deletion of class B services, billing information, and removal of time limits on Morale Calls.

1. Unit Commander's Responsibilities.

1.1. Ensure their organization complies with this instruction.

1.2. If unit Commander Support Staff (CSS) personnel will not be acting as Cybersecurity Liaisons (IAW AFI 33-200 to become AFI 17-130), appoint in writing a Primary and Alternate Cybersecurity Liaison (CL) or Primary and Alternate Telephone Control Officer (TCO) to manage the unit's communications requirements. Appointment letters must be submitted to the Wing Cybersecurity Office (WCO).

1.3. Be responsible for DSN and commercial toll calls placed from their unit.

1.4. Appoint, in writing, a list of individuals authorized to place routine long distance calls and send it to 35 CS/SCOIN.

1.5. Support Cyber Readiness measures and requests as part of the Wing's CRP.

2. Wing Cybersecurity Responsibilities.

2.1. Be the focal point for ensuring unit TCOs/CLs comply with this instruction.

2.2. Train all TCOs/CLs on program related duties.

2.3. Maintain the unit TCO/CLs training and guidance, ensuring it is up to date and current.

2.4. Be the Cyber Readiness focal point for the installation and ensure the requirements of the 35 FW/CC, 35 CS/CC and MPTO are met as well as develop necessary requirements and procedures to ensure CRP success.

2.4.1. Appoint a CRP Manager (recommended E-7 or above) and team with the PACAF A36IS provided contractor to develop/maintain the CRP.

2.4.2. Conduct monthly meetings with the 35 CS/DO and all primary CRP area POCs, and track the overall cyberspace posture for the Wing.

2.4.3. Once a quarter, ensure the 35 CS/CC attends the monthly meeting and at a minimum cover every gradable area of the DISA CCRI.

3. TCO Responsibilities

3.1. Serve as a liaison between their organization and the 35 CS for telephone related issues.

3.2. Be appointed, in writing, by their organization commander or equivalent.

3.3. Complete training provided by the WCO. TCOs will need to contact the WCO to request training material within 30 days of appointment.

3.4. Request a WOMS account for submitting change requests and work orders to the 35 CS for processing. A WOMS account will not be authorized until a TCO appointment letter has been received by the WCO and the TCO has completed the applicable training.

3.4.1. If a TCO cannot be given a WOMS account due to lack of an Air Force network account, they should submit all new requests to the 35 CS/SCXP utilizing an AF Form 3215, *Base Communications Request*.

3.5. Complete an annual inventory of all assigned telephone lines in their unit, as well as applicable CDA actions (refer to AFI 10-712). Once completed, the telephone line and CDA inventories will be submitted to the WCO organizational e-mail box (**35fw.ia@us.af.mil**). If unneeded lines are discovered, submit a WOMS or AF3215 request to disconnect them.

3.6. Coordinate with unit RAs or equivalent for billing matters as required.

4. Cybersecurity Liaison Responsibilities

4.1. Complete CL training within 30 days of being identified by the WCO.

4.2. Request a WOMS account for submitting change requests and work orders to the 35 CS for processing. A WOMS account will not be authorized until WCO verifies and the CL has completed training.

4.3. Complete an annual inventory of all assigned telephone lines in their unit, as well as applicable CDA actions (refer to AFI 10-712). Once completed, the telephone line and CDA inventories will be submitted to the WCO organizational e-mail (**35fw.ia@us.af.mil**). If lines are discovered that are no longer needed, a WOMS request will be submitted to disconnect lines.

5. 35 CS Billing Office Responsibilities

5.1. Ensure that all unit RAs receive their bills and call details on a monthly basis via SharePoint, or by e-mail directly to unit RAs.

5.2. Process Communications Service Agreements (CSAs) for requirements that involve billing. This includes, but is not limited to iPhone/cell phone requests, iPhone/cell phone terminations, iPhone/cell phone accessories, iPhone/cell phone replacement, iPhone/cell phone transfers, billing plan changes, commercial lines, and other actions related to billing. This applies to appropriated funds agencies only.

5.3. Work with all unit RAs or equivalent to ensure all bills are paid on time.

5.4. Serve as a liaison between the 35 CS and local commercial telephone agencies for billing.

5.5. Use the operator compiled list of long distance, mission essential telephone calls to ensure the appropriate unit is billed for the expense of the call.

6. Base Operator Responsibilities

6.1. Collect relevant information from users placing long distance, mission essential phone calls.

6.1.1. For all other mission essential, long distance phone calls, the operator will annotate the name, rank, unit and DSN number of the individual placing the call.

6.2. Send the lists monthly to the 35 CS Billing Office for verification and billing purposes.

6.3. Maintain the base digital phone directory. All requested changes to the phone directory should be made through the operator (35 CS/SCOIN).

7. Unit RA (or Equivalent) Responsibilities

7.1. Budget for and ensure funds are loaded to pay units phone bills on time.

7.2. Process all CSAs required for communications support of their unit.

7.3. Perform the monthly toll call verification with the 35 CS Billing Office as needed.

8. Control of Defense Switched Network (DSN) and Commercial Toll Calls.

8.1. Use of DSN and commercial toll calls is authorized for command elements and agencies requiring long-distance telephone communications support of their mission and is restricted to essential official calls requiring timeliness that cannot be achieved by other means (i.e., official or electronic mail). The length of a call is limited to the minimum time required to conduct the official business. Commercial long-distance calls for personal matters are strictly prohibited. Please refer to **http://www.disa.mil/Network-Services/Voice/SBU-Voice/Using-DSN/DSN-Tutorial/Toll-Free-Commercial-Calls.**

8.1.1. All requests for "99" commercial access will be submitted in WOMS or other locally approved method with required attachments. Attachments include a memorandum signed by the requesting Unit Commander vouching for the mission need as well as a breakdown listing the telephone number, LEN number, and justification for each telephone requiring the service. These documents must be submitted by the CL or TCO.

8.1.2. For all other individuals needing to place an essential official long distance telephone call, the Base Operator will annotate the name, rank, unit and DSN number of the individual placing the call for telephone billing purposes prior to authorizing the call. Each month the Base Operator will report the compilation of each units calls to the 35 CS Telephone Billing Office for billing.

8.2. Long distance callback services will not be used from official base telephones. All service agreements at Misawa Air Base are restricted to "Customer-to-Company" only. All problems with service will be handled between customers and the service provider. There are no exceptions or waivers to this rule.

9. Trouble Ticket (Remedy)

9.1. For communications services interruptions, unit members will call 315-226-2666, option 9 or utilize the Misawa Comm Focal Point (CFP) Org Box to report the outage to the Communications Focal Point (**misawa.commfocalpoint@us.af.mil**).

9.2. Any open ticket will be classified as Critical, High, Medium, or Low priority. The matrix below depicts general guidelines for the standard level of service provided by AFNetOps. Escalations of outages that include mission impact are generally classified SECRET. For this reason, all effort should be made to provide escalations via secure means; however, for after-hours notifications, or if secure communications are not available, unclassified notifications may be made.

Table 1. Trouble Ticket Priority Matrix.

Service Request Priority	Examples	Response Time/Update/Monitor
Critical	Any core service outage affecting multiple bases; Critical Core Service; Outage having a critical impact on AFNet C2 capabilities; direct combat support system failure; service interruption resulting in potential loss of life; POTUS support; DRSN Outage; CAT I (Root Access), CAT II (User Access), CAT IV Denial of Service), CAT VII (Major Virus) events.	Immediate/4 Hours/24 X 7
High	Base isolation; base-wide core service outage; any outage affecting a VIP; CMI (do not report above Secret).	30 Mins/8 Hours/24 X 7
Medium	Hazard Conditions (HAZCON); Issue(s) causing work-stoppage affecting multiple users (whole offices, floors, buildings); degraded base-wide network capabilities. CAT III (Attempted Access), CAT VI (Scan/Probe), CAT VII (Minor/Contained Virus), CAT VIII (Unconfirmed) event.	1 Hour/24 Hours/Daily
Low	Event causing single-user/client work stoppage; routine end-user ticket; intermittent problems.	24 Hours/2-5 Days/Every 5 Days (Auto-escalate after 10 days to Medium)

10. WOMS priority

10.1. All requests submitted will be put into one of the following categories:

10.1.1. Enhancement: Use for items that will enhance capabilities, but are not required for continued support of the mission.

10.1.2. Required: Use for items that, if not approved, may result in some kind of delay or work stoppage, but are not truly mission critical.

10.1.3. Mission Critical*: Use for items that, if not approved, will result in a CRITICAL mission work stoppage that could cause a serious degradation of capability resulting in catastrophic loss of money or time. **NOTE:** Completion of WOMS requests will depend on a number of factors to include: workload, priority, available resources and feasibility. The 35 CS will work with TCOs and CLs to keep customers abreast of WOMS status. **NOTE*:** TCOs/CLs will be required to submit a justification letter for Mission Critical WOMS requests. At a minimum, the justification letter must state why the WOMS request is mission critical, why the WOMS request was not submitted in a timely manner, and must be signed by the Unit Commander or equivalent.

11. WOMS Ticket Expiration

11.1. To ensure WOMS tickets are accomplished and unnecessary tickets closed, customers (ticket submitters) will have 30 days to act on a ticket that has been assigned back to them from a work center.

11.2. After a work center assigns the ticket back to a customer, an email will be sent to the CL as well as the customer informing them of the ticket assignment.

11.3. A second email will be sent by the office who is responsible to the CL and customer at the midway point if no response is received.

11.4. After 30 days of no action by the CL or customer, the ticket will be closed by 35 CS/SCXP.

12. Communications Equipment Accountability

12.1. Unit Information Technology Equipment Custodian(s) (ITEC) will follow AFMAN 17-1203, Information Technology (IT) Asset Management (ITAM), para 1.2.14 for processes/procedures and work with the TCO/CL to submit a WOMS request for approval of all new accountable communications equipment purchases. Once purchased, the assets will be shipped to the Information Technology Asset Management (ITAM) office to be added to a unit ITEC account. These assets include, but are not limited to, desktops, laptops, monitors, servers, routers, printers, digital senders and Voice over IP (VoIP) phones. Questions regarding approved devices, shipping address, or what constitutes an accountable asset will be directed to the ITAM office.

12.2. Unit ITEC(s) will turn in all excess or broken accountable communications equipment according to ITAM office guidance. All classified/unclassified Hard Disk Drives (HDD) will be brought to the ITAM office for sanitization prior to turn in.

13. 35 FW Cyber Readiness Initiative: Purpose. While a goal of this program is to provide continuous measurement and monitoring of cyberspace threats using DoD Command Cyber Readiness Inspection (CCRI) criteria, maintaining and tracking the overall security posture and impact to operational readiness of cyberspace is the primary focus. The Commander's Intent for this initiative is to institutionalize sustainable, repeatable processes, training structures, and policies that result in a cyber terrain that balances security with mission assurance at all echelons.

13.1. Scope. The local Cyber Readiness Initiative will utilize DISA Phase 4 CCRI Grading Criteria IAW instructions set forth in USCC TASKORD 14-0290 and enforced through MPTO 00-33A-1109.

13.2. Process. Success of the Cyber Readiness Initiative is achieved through a 4-step process flow (Assess, Score, Remediate, and Manage Changes) in an effort to organize activities across several work centers. Cyber Readiness is assessed and tracked across three major areas:

13.2.1. Contributing Factors. The Contributing Factors areas are designed to assist in evaluating the Command's emphasis on compliance of the Information Assurance (IA) Controls that are in place at a site during a CCRI. The inspection items/questions in this document are linked to one or more of the IA Controls found in NIST SP 800-53. The Contributing Factors area evaluates three overall IA areas: Culture, Capability, and Conduct.

13.2.2. CND Directives. The Computer Network Defense (CND) Directives areas are designed to provide guidance for completing the USCYBERCOM CND Directives such as Communications Tasking Orders (CTOs), Warning Orders (WARNORDs), Task Orders (TASKORDs), Operations Orders (OPORDs), and Fragmentary Orders (FRAGOs) for the Compliance Report during a CCRI.

13.2.3. Technology Areas. The Technology Areas are designed to indicate a site's compliance to any published Security Technical Implementation Guide (STIG) for the Internal Network.

14. Cyber Readiness Roles and Responsibilities. Cyber Readiness support personnel will comply with assigned roles as designated in this operating instructions and through the Accountable, Responsible, Support, Consult and Inform (ARSCI) responsibilities matrix. The WCO will be the OPR for the ARSCI matrix located \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

14.1. Cyber Readiness Responsible Action Officers (RAOs)

14.1.1. Cyberspace operations are at the center of the process as each work center shall assign a primary and alternate designated as a RAO from the following sections: CS/SCOI (NETMAN), CS/SCOO (NCC), CS/SCOSC (CFP), CS/SCOST (CST), CS/SCXP (Plans), CS/SCQ (QA), CS/SCXS (WCO), FW/IP, and all Functional System Administrators/System Program Offices (FSA/SPO) located on Misawa AB, Japan.

14.1.2. Each section will:

14.1.2.1. Assess each area under purview using manual or automated audit checklists provided by DISA and/or this program.

14.1.2.2. Compile results from their checklists, score, and posts their results in the appropriate trackers/spreadsheets (\\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists) as required showing progression of Contributing Factors, CND Directives and Technology Areas.

14.1.2.3. Mitigate efforts by developing POA&Ms from audits and creating a priority matrix on all open findings tracking progression for fixing/closing items. Efforts will be annotated in the comments section, comments can include but not be limited to i.e. estimation closeout date, progression towards to fixing/closing items, contacting another Tier, etc.

14.1.2.4. Re-score efforts tracking updates and changes on a monthly basis by deadline set by the WCO for group briefs.

14.1.2.5. Manage any and all changes when new STIGs/IAVMs are published (check monthly).

14.1.2.6. Ensure all personnel key players are present for monthly briefs conducted by the WCO.

14.2. CS/Wing Cybersecurity Office (SCXS)

14.2.1. Provide oversight and management of the local CRP.

14.2.2. Provide quarterly reoccurring Cyber Readiness status briefing to the CS/CC.

14.2.3. Conduct continuous monitoring and auditing of the security posture of the network.

14.2.4. “Document and socialize standardized, repeatable processes, procedures, and products across all [individual work centers involved] cyberspace organizations which engage in cyber [readiness] space surety activities." (MPTO 00-33A-1109).

14.2.5. Conduct periodic STIG training to Cyber Readiness support personnel.

14.2.6. Develop local guidance as necessary to ensure success of the program.

14.3. CS/Cyberspace Plans and Programs (SCXP)

14.3.1. Provide CRP requirements tracking.

14.3.2. In coordination with the ISSM and WCO, utilize change management (CM) processes to manage changes resulting from security audits conducted across the network.

14.3.3. Conduct change control review board (CCRB) meetings at least once a month and post meeting minutes of all approved and non-approved changes of the network.

14.4. CS/Quality Assurance (SCQ)

14.4.1. Conduct validation activities to ensure CRP objectives are being met.

14.4.2. Review and verify POA&Ms, CND audits (checklists), and applicable STIGs on a quarterly basis to validate accuracy. Discrepancies shall be corrected by the responsible work center in coordination with the ISSM.

14.5. Wing Information Protection office (WG/IP)

14.5.1. Work in coordination with the CS appointed Traditional Security POC to provide answers to the Traditional Security STIG on a quarterly basis.

14.6. Program Management Offices/Functional System Administrators (PMOs/FSAs)

14.6.1. Provide monthly vulnerability scans (if not provided by the CS) and additional information on the security posture of computer assets under their purview. If reliant on the local vulnerability scanner, they must receive the results affecting their systems and mitigate vulnerabilities. A Service Level Agreement (SLA) for all PM systems must be completed and current.

14.6.2. Coordinate with CS Cyber support personnel and system owners to patch and update system vulnerabilities only upon approval of the PMO or system owner.

14.6.3. Ensure significant changes to a PM system baseline are vetted and approved through the CS CCRB.

14.6.4. Attend monthly PMO meetings as provided by SCOO respective CS appointed POC.

15. Assessment and Scoring Procedures

15.1. Contributing Factors - Capability

15.1.1. Assessment: This is part one of a three part series of manual checks assessed using the Contributing Factors checklists provided on the network shared drive (\\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\1 - Contributing Factors) against the following five indicators:

Table 2. Contributing Factors - Capability Assessment Matrix.

Indicator	Criteria	Responsible Action Officer(s)
Has the site properly aligned with a CNDSP and leverages those capabilities?	• Site is aligned with a certified Tier II CNDSP - to be considered "aligned", site must have both MOA in place and funded.	ISSM CNDSP
	• A fully executed MOA -OR- the DOD Component has designated the Tier II CNDSP that will support the site (documented).	
	• Roles and responsibilities of the supporting Tier II CNDSP and the site (Tier III) subscriber are documented and adhered to.	
	• Site has contact information and is aware of CNDSP support available and complies with reporting requirements (demonstrated).	
	• Tier II CNDSP is integrated into the incident reporting procedures.	
Has an external NIDS been deployed and is the CNDSP monitoring?	• NIDS is located on the wide area network side of the enclave boundary.	ISSM CNDSP
	• At a minimum the accredited Tier II CNDSP should have visibility to all external network traffic.	
	• If MOA and payment is in place, but no sensors, site must be providing feeds to supporting Tier II CNDSP which the Tier II is actively monitoring (must be verified	
Has an internal NIDS been deployed and is the command or CNDSP monitoring?	• NIDS has the appropriate architecture to monitor the interior side of the enclave boundary.	ISSM CNDSP
	• NIDS are under the control of the supporting Tier III organization (enclave level activity) OR there is a formal agreement in place with an accredited Tier II organization to monitor.).	
Has the local incident handling program been developed and exercised recently?	• Site has a documented cyber incident response plan.	ISSM
	• Site personnel are aware of the plan and implement it when necessary. *1. Verify the location of the incident handling program/plan and that it is the most recent version.*	SCOSC

	• After action reports, lessons learned, etc., exist showing the plan is exercised, reviewed, and updated as appropriate. *1. Verify these artifacts exist and are current.*	ISSM, SCOSC, SCOO
Does the site have an executable COOP that will sustain mission essential functions?	• An alternate site has been designated that will not be affected by the same manmade or natural disaster *1. Verify that an alternate has been designated in writing and is approved by CS leadership.*	SCOO
	• Backup and restoration assets are protected - *Verify that backups are occurring and that there is a plan for continued operation.* - *Verify that the protection measures are in place to include:* o *Physical location of backup asset (secure vault, controlled area, etc).* o *Access to backup software is accessible only to authorized sysad personnel.*	SCOO
	• Data backup is performed IAW security baseline and NIST SP 800-53, backups are protected and stored off site - *Verify the backup tapes are located in a fire rated GSA approved safe.* - *Verify that weekly backups are stored offsite.*	SCOO
	• An disaster plan exists that accomplishes restoration/transition of mission essential functions with the time period required IAW control baseline - *Verify the location of the Disaster Recovery Plan (DRP) and that it is the most recent version.*	SCOSC, ISSM, SCOO
	• Enclave boundary defense security measures at alternate site are equivalent to the primary site. - *Verify that the alternate site is located within or interfacing with the production enclave.*	ISSM

	• COOP and disaster recovery plans are exercised IAW with site's control baseline. - *Verify that the DRP have been exercised within 1 year and uploaded in eMASS.*	ISSM, SCQ
	• Mission essential functions are identified for priority restoration planning - *Verify that mission essential functions are identified in the DRP and/or COOP.*	ISSM
	• UPS or backup generators are configured to support key IT assets - *Verify designation of Key IT assets on the critical facility lists.* - *Validate the required generator testing is occurring on a monthly basis.*	SCOO, SCOI
	• Backups of critical software are available and protected - *Verify existence of critical software.* - *Verify backups are occurring if critical software exists.*	SCOO

15.2. Contributing Factors - Conduct

15.2.1. Assessment: This is part two of a three part series of manual checks assessed using the Contributing Factors checklists provided on the network share (\\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\1 - Contributing Factors) against the following five indicators:

Table 3. Contributing Factors - Conduct Assessment Matrix.

Indicator	Criteria	Responsible Action Officer(s)
Are administrators adequately trained to conduct IA functions (8570)?	• IA Workforce IAM and IAT level designations are consistent with the responsibility levels stated in DoD 8570, and covers military, government civilian, and contractor positions	SCXS
	• Site is at 100% with DoD 8570 Certification compliance requirements. (new employees have 6 months to reach certification)	
	• Computing environment certifications are maintained that relate to the primary duties of Information Assurance Technical professionals as required by their employing organization.	
	• IA or IA related training for privileged account holders (non-user level training) (e.g., firewall, incident handling, networking, SRR training, IAO/IAM courses)	
Are configuration management (CM) processes implemented and enforced?	• Chartered Configuration Control Board (CCB) (documented) that meets regularly	SCXP
	• Documented standard for configuration (e.g., STIG)	ISSM, SCO, PMO/FSA
	• IA membership in CCB	ISSM
	• Documented CM roles, responsibilities, and procedures to include a change control process that includes IA in review process	SCXP
	• Evidence that the CM process is enforced	ISSM
Does the site have a comprehensive vulnerability management program?	• Vulnerability Management Program addresses all vulnerabilities (not just IAVM) that endanger the confidentiality, availability, and integrity of the information and information systems	ISSM, SCO
	• System compliance is checked before being placed on the operational network *(i.e. Residual Risk report for new PM system deployments)* - *Verify that the most recent OS baseline is being loaded (i.e. "Frankenstein image").*	ISSM, SCXP, SCO
	• System baselines are maintained and updated - *Verify that patches are deployed with specified timeline.* - *Ensure no open vulnerabilities older than 30 days*	SCO

	(without a POA&M on file).	
	• Compliance standards are stated and enforced on both local owned, PM and rider systems - *Verify that the DISA approved baseline for ACAS, HBSS and other IA Enabled products are deployed onto the network.*	ISSM, SCO, PMO/FSA, 561 NOS
	• There is an effective connection approval process that extends the vulnerability management standard, accountability and reporting to all organizations gaining connectivity through the site's connection to the DoDIN	CNDSP
Are vulnerability management processes consistent and repeatable?	• TASKORD 13-0670 compliance	ISSM
	• Rigorous scan – analyze – patch – scan methodology	ISSM, SCOO
	• Entire IP space is covered by automated scans and patching at least monthly - *Verify appointment letter is recent and has the entire IP space captured.*	ISSM, SCOO
	• Full Safe scan policy is used (if additional policies are specified by USCYBERCOM, they are included too)	SCOO
	• 95+% administrative access on all targets	SCOO
	• All domain and non-domain systems are scanned and patched	SCOO
	• Automated patching capabilities are used for primary OS/Applications and all third party software	SCOO
	• Policy and procedures addressing a removable hard drive environment and deployable/traveling systems are developed and enforced – readiness of these systems is consistent with the garrison network and within acceptable CCRI ranges	ISSM, SCOO
	• Trend analysis is conducted and shows remediation is effective over time	ISSM, SCOO
	• No high occurrences of Critical or High vulnerabilities over 30 days old	SCOO
Have identified vulnerabilities been addressed immediately?	• Site takes quick fixes for action that have already been approved, but missed on some systems	ISSM, SCXP
	• Site addresses unapproved/untested fixes via their local CM process, but with a high priority	ISSM, SCOO, SCXP
	• Vulnerabilities that cannot be fixed quickly are identified to the IAO/ISSM/AO and mitigation options presented (i.e. POA&M via 690 NSS/AMAC)	SCOO, PMO/FSA

15.3. Contributing Factors – Culture

15.3.1. Assessment: This is part 3 of a three part series of manual checks assessed using the Contributing Factors checklists provided on the network share (\\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\1 - Contributing Factors) against the following five indicators:

Table 4. Contributing Factors - Culture Assessment Matrix.

Indicator	Criteria	Responsible Action Officer(s)
Is command leadership (O-7/SES, O-6/GS-15) fully engaged in the Cybersecurity program?	• Command leadership is kept informed of Cybersecurity program status via Cybersecurity/CND updates, IAVM/CTO compliance tracking reports, Stand-up Briefs / Operations Updates, Cybersecurity/CND Dashboards, Internal / External assessments.	ISSM
	• Command leadership and AO involvement in CCRI preparation and execution	Flight/CC, ISSM
	• Command leadership and AO awareness of the current security state of the networks and enclaves	CS/CC, ISSM
	• Command leadership has awareness of their supporting Intel organization.	CS/CC, ISSM
	• Command leadership receives cyber related Intelligence/Threat Briefings from their supporting Intel organization.	CS/CC, ISSM
Are administrators aware of and implement STIG/Benchmark requirements?	• Administrators are aware of and know where to access the STIGs, NSA Guides, and any CC/S/A specific security guidelines (Demonstrated).	SCO PMO/FSA ISSM
	• Administrators reference the above mentioned guides when performing their Cybersecurity responsibilities (Demonstrated).	SCO PMO/ISSM ISSM
Does Site have an Authority to Operate (ATO) for the circuit being inspected and is it current?	• An ATO/IATO signed by the current AO is available	ISSM
	• Has a plan for ensuring that the ATO/IATO and ATC/IATC is renewed prior to expiration of their current approvals.	WCO
	• Site begins working on renewing the ATO at least 90 days prior to the expiration.	WCO PACAF/A36IS AFSPC/A6
Do approved POA&Ms exist for the over 80%	• POA&Ms are feasible and approved by the DAA	ISSM, SCO
	• POA&Ms include mitigation factors that have been implemented	SCO, PMO/FSA

of vulnerabilities discovered during the CCRI?	• POA&Ms are documented	ISSM SCO, PMO/FSA
	• POA&Ms include a fix date for when the vulnerability will be remediated	SCO, PMO/FSA
Are PM system baselines established and maintained IAW PM Guidance?	• Configuration Management of the PM system baselines is consistent with risks identified and accepted by the system AO for the PM System.	ISSM PMO/FSA SCO
	• PM Baselines observed adhere to the TFM and patch releases approved by the PM	PMO/FSA, SCO
	• Site has contact information for the PM and can access websites distributing information and updates for the PM systems	SCO
	• Site can demonstrate the process they use to check for updates and have evidence of "keeping in touch" with the PM Office	SCO
	• ACAS asset lists and results for PM systems are organized and managed to facilitate adherence of the baseline	SCO, PMO/FSA
	• Residual risk was documented and considered by the AO prior to allowing the PM system on the network	ISSM, PMO/FSA, SCO
	• Mitigation actions directed or recommended by the PM are in place and enforced	SCO, PMO/FSA
	• No Critical Concern indicator received on any PM vulnerability scan or technology review during CCRI	PMO/FSA, SCO
	• Administrative Access is gained to over 95% of PM systems	SCO

15.4. Baseline Scoring and Documentation for Contributing Factors

15.4.1. Final results of assessment is recorded on the Cyber Readiness Master Tracker by the WCO located on the network share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\6. Master Tracker.

15.4.2. Each RAO is required to update and reflect personnel or policy changes in the ARSCI as part of assessment closeout procedures on the network share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

15.5. Sources

15.5.1. Contributing Factors Guide located at the DISA CCRI Program website (**https://disa.deps.mil/ext/cop/fs-ccri/inspections/CCRIPAGES/CCRI%20PHASE%20IV.aspx**).

16. CND Directives

16.1. Assessment: Using checklists provided on the network share \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\2 - CND Directives, the RAO will conduct a manual assessment against the following eleven indicators:

Table 5. CND Directives Assessment Matrix.

Indicator	Criteria	Responsible Action Officer(s)
FRAGORD 1 to OGS / CTO 07-15 PKI PHASE II	a. Digital Signature Policy - there must be a policy created and in use IAW CTO 07-15 PKI Phase II, Task 1. *1. The RAO shall assess compliance by choosing 5 random users and have them test whether or not those individuals are able to ss or links without a digital signature when selected to do so. If the test allows for an attachment to be sent without a digital signature when selected to do so, this is a finding.*	AF AO SCOSC
	b. User Based Enforcement (UBE) - All Windows Active Directory accounts must use Common Access Card (CAC), Personal Identify Verification (PIV) compliant hardware token, or Alt-token (ALT) and the "Smart card is required for interactive logon" must be enabled. - *Checklist procedures: In order for this category to be "Compliant", All Windows Active Directory accounts must use Common Access Card (CAC), Personal Identify Verification (PIV) compliant hardware token, or Alt-token (ALT) and the "Smart card is required for interactive logon" must be enabled IAW CTO 07-15 PKI Phase II , or fully documented in step X.X.X below.* - *The policy is applied through organization Group Policy in Active Directory managed by the 561 NOS. The RAO shall assess compliance by choosing 5 random user accounts. If an Active Directory (AD) server is not reviewed, review the organizations policy of account creation to ensure UBE is required. If an AD server is reviewed, use the following procedure to check a sample of accounts.*	SCOSC

	c. User/password Accounts - all Windows Active Directory accounts are either UBE or are documented IAW CTO 07-15 PKI Phase II, Task 6. - *All non-UBE accounts must be approved through the Two-factor Authentication (2FA) exemption template located on the 690 COG website https://org1.eis.af.mil/sites/67cw/690cog/690%20NSS/TwoFactorAuthentication/*	SCOSC
	d. Password Security Measures - either the site is 100% UBE or DoD password security requirements have been met IAW CTO 07-15 PKI Phase II, Task 3. *1. Checklist procedures: In order for this category to be "Compliant", either the site is 100% UBE or DoD password security requirements have been met IAW CTO 07-15 PKI Phase II, Task 3. If password security requirements have not been met, then the site is "Not Compliant".* *2. Password security requirements can be found in this CTO as well as consist of the following items:* *1. NETMAN password requirements on ACS can be found here: \\QKKG-FS-022V\SCO\SCOI\SCOI - NETMAN\03 - Standard Operating Procedures\NETMAN SOPs CR365*	SCOO / SCOI
	e. Soft Certs - verify removal of all software certificate installation files (.p12 or .pfx) IAW CTO 07-15 PKI Phase II, Task 4. *This assessment applies to local online storage assets connected to network (servers, workstations, printers, phones, hard drives) IAW CTO 07-15.* - *Checklist procedures: In order for this category to be "Compliant", verify removal of all software certificate installation files (.p12 or .pfx) from hard drives and any other online storage devices IAW CTO 07-15 PKI Phase II, Task 4.* - *This task is a perpetual task with a recommended frequency of searching for these file types at least weekly. The site should have a documented process for this or can demonstrate via the use of a search or find. If .p12 or .pfx certificate installation files are found the site is "Not Compliant".*	SCOO

	f. Public Key Encryption (PKE) Servers - all web servers are PKE enabled except for external servers containing only data approved for public release. *This assessment applies to local assets (QKKG-WS-PEX2P) IAW CTO 07-15.* - *Checklist procedures: In order for this category to be "Compliant", all web servers are PKE enabled. An exception to this directive is external web servers containing only data approved for public release IAW FRAGO 1 Tab E to Appendix 3 to Annex C to OGS, Paragraph 3.C.1.C.* - *If any exist that are not PKE enabled or data not approved for public release is available on external facing servers that are not PKE enabled, it would be marked "Not Compliant". 52QKKG-TMG-001v & 52QKKG-TMG-002v are controlled at NOS level.*	SCOO
	g. DOD IA Awareness User Training - *Have the base training manager pull an ADLS report shows DOD IA Awareness Stats.*	WCO
TASKORD 12-0863 SIPRNET PKI	• User Based Enforcement (UBE) - All Windows Active Directory accounts must use Common Access Card (CAC), Personal Identify Verification (PIV) compliant hardware token, or Alt-token (ALT) and the "Smart card is required for interactive logon" must be enabled. *This assessment applies to local assets for implementation of email digital signature plan IAW CTO 06-02.* - *Checklist procedures: In order for this category to be "Compliant", All Windows Active Directory accounts must use National Security System (NSS) PKI hardware tokens for cryptographic network logon.* - *If an Active Directory (AD) server is not reviewed, review the organizations policy of account creation to ensure NSS PKI hardware tokens are required. If an AD server is reviewed, use the following procedure to check a sampling of accounts.*	SCOSC
	• All accounts (both Windows and non-Windows accounts) are either UBE or documented (to include	SCOSC

	temporary exception users).	
	• Password Security Measures - either the site is 100% UBE or DoD password security requirements have been met.	SCOSC
TASKORD 13-0670 IMPLEMEN-TATION OF ACAS	• Monthly Scan - The site must conduct the monthly scans of all active IP ranges. Every asset with an IP address in these ranges must be included. *Checklist procedures: In order for this category to be "Compliant", the site must conduct the monthly scans of all active IP ranges.* - *Every asset with an IP address in these ranges must be included. If the entire IP ranges are not scanned at least monthly or scanned with incorrect configuration, then the site is "Not Compliant".* - *Evidence of monthly scans can be found from the completed scans within Security Center or a Tier 2 data repository that scan results are uploaded to at least monthly. The review of these indicators must confirm that monthly scans of existing networks have occurred consistently throughout the 90 day period prior to the inspection.*	SCOO
	• Scan Tool -the site must have ACAS implemented on site. If a different scanner other than ACAS is in use, the site must provide an ATO and a contract support with the vendor. - *Checklist procedures: In order for this category to be "Compliant", the site must have ACAS implemented or if utilizing a different vulnerability scanner the site must provide a Service/local Authorizing Official (AO) Authority to Operate (ATO) and a contract of support with the vendor in order to be compliant. If no vulnerability scanner is used or the above criteria for not ACAS scanner is not meet, the site is "Not Compliant".*	SCOO
	• Configuration - ACAS must be configured accordingly - *Retrieve the latest version of STIGs, IAVMs and Policy checklists along with STIG viewer from the following website (http://iase.disa.mil/stigs/Pages/index.aspx)*	SCOO

OPORD 12-1016 HBSS & TASKORD 14-0305	• ePO baseline (N/A for Misawa) *This assessment does not apply.*	SCOO
	• Point Product Deployment (> 95% for full compliance) - *This assessment applies to McAfee Agent, Host Intrusion Prevention (HIP), Policy Auditor, Data Loss Prevention and Rogue System Detection IAW OPORD 12-1016.* - *Create POA&Ms for the following categories: McAfee Agent, HIP, Policy Auditor, Data Loss Prevention and Rogue System Detection. Refer to paragraph 18 for POA&M instructions.*	SCOO
	• Client Configuration	SCOO
	• Rogue System Detection (RSD) (> 95% coverage for full compliance) *This assessment requires two RSD sensors per subnet.* - *RSD coverage is a coordinated effort between the NCC and the 561 NOS.*	SCOO
	• Rollup reporting (N/A for Misawa)	561 NOS
	• HBSS Training (N/A for Misawa)	561 NOS
TASKORD 14-0185 Insider Threat Mitigation (SIPRNET only)	**• Data Transfer Authorized Users (AO Approved)** *This assessment applies to local assets on the SIPRNet Domain for implementation of authorizing official approved users to transfer media from the SIPRNet environment via removable media IAW CTO10_084 and 10_133* *Checklist procedures: In order for this category to be "Compliant", the site must adhere to the following:* - *Ensure all users and systems that require data transfer activity complete the necessary waiver and follow all instructions to secure functionality. These waivers are approved by the site's Authorizing Official (AO) of the rank of O-6 or higher, in writing to the ISSM when no other option for data transfer exists to support their mission requirement (e.g. CDS, networked backup server, etc).* - *Local SOPs and checklists are found here: The process is outlined and documented with an SOP and process that can be found in \\QKKG-FS-*	ISSM

	022V\SCX\SCXS\SCXSI\1. COMPUSEC\EPSEC-1 Removable Media\2. SIPR & NIPR Waivers\1. SIPR Removable Media. - *Document results: Approved waivers will be logged in the Unit's respective folder in the \\QKKG-FS-022V\SCX\SCXS\SCXSI share. Evaluation results shall be scored in the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing. This spreadsheet is located on the Cyber Readiness share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\2 - CND Directives.* - *Remediate/Track Progress: No mitigation or remediation actions need to be taken for this task. Waivers must be reviewed and re-accomplished 1 year after date on waiver, or functionality will be terminated.*	
	1. Removable Media Policy and Inspections 2. *3. This assessment applies to local assets on the SIPRNet Domain for implementation of removable media policy and inspections IAW TaskOrd 14-0185.* *4.* - *Checklist procedures: In order for this category to be "Compliant", the site must be utilizing the following:* - *The AO must develop organizational procedures for compliance with removable media. These procedures are covered in the removable media waiver as well as CTO 10_084 and 10_133.* - *The ISSM/Cybersecurity will conduct random quarterly inspections on all locations and users that have SIPR removable media capabilities. Inspections will focus on ensuring that required monthly logs submitted match up with the processes and procedures of authorized devices/individuals. Transfer frequency must correspond to requirements laid out in approved waiver.* - *Remediate/Track Progress: Discrepancies found between transfer logs and requirements/procedures will be treated on a case-by-case bases. Any*	ISSM

	indication of classified spillage/incident will follow incident response procedures outlined in the Misawa AB Incident Response plan, as well as 35 FW Operating Instruction (OI) 16-1400.	
	• Data Transfer Records/Auditing Removable Media (Monthly)	ISSM
	- *Thresholds for authorized use of removable media must be established to include, at a minimum, multiple attempts to use removable media within a 48 hour time period by individual authorized users and administrators.*	AF AO
	- *Investigations must be conducted on authorized users and administrators who exceed the established thresholds.*	IG
	- *The ISSM or AO shall report initially identified incidents where DoDIN usage exceeds designated thresholds and/or is initially identified as inappropriate or otherwise excessive to the appropriate LE/CI element and USCYBERCOM within 72 hours.*	ISSM
	- *At least one type of two-stage control for transfers of data from all DoD secret information networks to systems of lower classification.* - *Misawa Incident Response plan is updated (as necessary) and reviewed at least annually. This incident response plan must also contain response procedures for unauthorized data transfers. These response procedures are outlined in the Data Transfer IRP AAR and need to be updated parallel to the Incident Response Plan, and signed by the ISSM.*	CLs
	• **Disable "Write" Permissions for Removable Media – Data Loss Prevention (DLP)** a. Ensure all devices that are capable of installing the HBSS component, DLP (or Device Control Module [DCM]), are installed and all others that are not capable if DLP have an alternate means to disable data transfer activity (DTA) on SIPRNet assets. The DLP or DLP-like solution must also log all removable media activity and alert on all user of removable media. *This assessment applies to local assets on the SIPRNet*	SCOO

	Enclave for implementation of disable "write" permissions for removable media IAW CTO 06-02. *1. Checklist procedures: In order for this category to be "Compliant", the site must be utilizing the following:* *2.* *3. Email 561/NOS HBSS for ePO screenshots (Bi-annually) of approved SIPR Removable media exemptions. This is to verify that only approved users have exemptions in HBSS. DLP deployment will be verified by section 17.4.2.5.2 IAW OPORD 12-1016.* *4.* - *Keep a log of all screenshots saved for Records. Evaluation results shall be scored in the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing. This spreadsheet is located on the Cyber Readiness share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\2 - CND Directives* - *Any machines/users that are identified in provided screenshots that do not have an approved waiver must be removed from the exemption list immediately. This can be accomplished by opening a ticket with 561st NOS/HBSS to remove these machines and/or users. Upon completion, log ticket traffic for records.*	
	• **Privileged User Review** a. Process in place; Ensure site has a process in place for granting privileged user access regardless of network(s) on which they have privileged access. - *This assessment applies to administrator privilege accounts IAW CTO 06-02.* - *Checklist procedures: In order for this category to be "Compliant", the site must be consider:* - *Users requesting privileged user roles/accounts must have the following: DD Form 2875 for admin privileges, Completed Privileged User Agreement, and Proof of 8570 cert.*	ISSM

	- *Quarterly Review Check: (ISSM/WCO) Admin Accounts current and active, 8570 cert, current and valid security clearances, number of private accounts, and audit logs maintained.* - *Local SOPs and checklists are found here: \\QKKG-FS-022V\SCX\SCXS\SCXSI\9. Policy and Regulation\3. Local Policy* - *Remediate/Track Progress: Any vulnerabilities/items of non-compliance will be annotated on MFR and actions will be taken to disable, delete, or suspend and Administrative accounts as necessary. Progress will be tracked quarterly, and on a cyclical basis.*	
	b. Quarterly Review; Reviews must be conducted quarterly to ensure they have a continuing need for privileged capabilities or access.	ISSM / Unit Security Manager (USM)
	c. Clearances valid; Verify that the quarterly review includes validation of current from Security Manager (quarterly) - Privileged User info provided to Security Manager at least quarterly for re-verification - Action of users without clearance requirement (removal, waiver, etc) - Privileged users with waivers on file should be reviewed quarterly - Minimum use of waivers for minimum security clearance requirements	ISSM USM
	d. Number documented; Number of privileged users must be documented and provided.	ISSM / CFP
	e. Audit logs maintained; Privileged user audit logs must be maintained.	561 NOS
	1. **Privileged User Roles** a. Ensure site has conducted a review of privileged user roles. The site must define privileged user roles, ensure they align with Ref Q (DoD 8570.01M) and that all privileged users are assigned to a defined role. Total number of privileged users and how many privileged users hold multiple roles for SINGLE systems must be documented.	ISSM USM

	b. Site must have evidence that documents organizational and system actions that have been taken to minimize the number and scope of privilege for these (privileged) users. When possible, ensure role assignments are distinct and minimize roles and role assignments that allow root access.	ISSM USM
	c. Ensure audit data relating to privileged users actions is stored beyond the reach of those users and audit access to that data, evidence must be provided and may need to be validated with the Windows/UNIX reviewer. *This assessment applies to all privileged user accounts IAW DoD 8570-01-M.* *1. Checklist procedures: In order for this category to be "Compliant", the site must consider the following tasks:* *2. Ensure site has conducted a review of all privileged user roles. The site must define privileged user roles, align with Ref Q (DoD 8570.01M), and all privileged users are assigned to a defined role. Total number of privileged users and how many privileged users hold multiple roles for SINGLE systems must be documented.* *3. Audit data cannot be accessed by Privileged users, logs must be maintained by servicing NOS/AMAC.* *4. Local Privileged User Roles and Process MFR: \\QKKG-FS-022V\SCX\SCXS\SCXSI\Cyber Readiness Docs..* *5. Privileged users roles identified by DMDC Reports, sent weekly from PACAF. Locally updated on "8570" Tab on the Master Tracker: \\QKKG-FS-022V\SCX\SCXS\SCXSI\8. 8570.* *6. WCO ensures documents are updated quarterly parallel the Admin reviews.* *7. Document results: Evaluation results shall be scored in the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing. This spreadsheet is located on the Cyber Readiness share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber*	690th COG

	Readiness\1. Checklists\2 - CND Directives. *8. Remediate/Track Progress: Any vulnerabilities/items of non-compliance will be annotated on MFR and actions will be taken to disable, delete, or suspend and Administrative accounts as necessary. Progress will be tracked quarterly, and on a cyclical basis.*	
	Training and Incident Handling a. Ensure that the procedures to identify, report, and investigate violations of data transfer activity are documented in the site's Incident Handling Program and there is evidence that these procedures have been previously executed. The documentation must also include reporting to senior leadership of any violations.	ISSM USM
	b. Ensure that the acceptable use and approval process for use of removable media is included in the site's Network User Training Program. It should document what devices are allowed to be connected to an asset as well as the process to achieve approval to conduct any data transfer activity on SIPRNet. *1. This assessment applies to training and incident response plan for unauthorized data transfers IAW CTO 06-02.* *2. Checklist procedures:* *3. Misawa Incident Response plan is updated (as necessary) and reviewed at least annually. This incident response plan must also contain response procedures for unauthorized data transfers. These response procedures are outlined in the Data Transfer IRP AAR and need to be updated parallel to the Incident Response Plan, and signed by the ISSM.* *4. Local documents are found here: \\QKKG-FS-022V\SCX\SCXS\SCXSI\Cyber Readiness Docs.* *5. Document results: Evaluation results shall be scored in the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing. This spreadsheet is located on the Cyber Readiness share at \\QKKG-FS-022V\ FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\2 - CND Directives.*	ISSM USM

	6. Remediate/Track Progress: Any incidents found must follow guidance in the documents mention in section 'C' and remediated thereafter. Store all subsequent reports and results appropriately depending on classification of information.	
	Sharing Portals a. Sharing Portal PKI; Ensure the site has reviewed information sharing portals (SharePoint, Shared drives, etc.) hosted on the SIPRNET to ensure they require authentication. Authentication shall require PKI-enabled access, per USCYBERCOM FRAGO 2 to TASKORD 12-0863, DoD SIPRNet Public Key Infrastructure Implementation, Increment One: Phase One and Two, 23 JUL 12.	ISSM SCXK
	b. Review all SIPRNet Web sites managed by the site by accessing the sites with a browser and ensure that they require PKI-Authentication, normally via a CNSS Token. This can be verified by going out the site-maintained sharing portals and ensuring PKI is required.	ISSM SCXK
	c. Shared Portal Identification; Site must provide proof that they have determined how many information sharing portals on the SIPRNET share classified information internal and external to their organization. Once sharing portals are identified, site must show that they have determined how many information sharing portals on the SIPRNET are openly accessible upon authenticating to the domain. This will be validated by using the site's list to access these portals and attempting access.	ISSM SCXK SCOO
	d. Sharing Portal Clean-up; Site must provide their strategy, developed with participation from all affected parties, to identify and remove from information sharing portals on the SIPRNET all particularly sensitive information that should not be shared with the full user population. *This assessment applies to local assets for implementation of sharing portals IAW CTO 06-02.* *1. Misawa does not have any SIPRNet hosted*	SCXK

	sharing websites online. Other sharing portals such as shared drive have access control measures in place that are maintained by security groups and permissions. Only users with a need to know should access to certain unit folders and information. *2. Checklist procedures: assessor will attempt to access a random folder/execute a file in a location where he/she does not have a need to know.* *3. Document results: Evaluation results shall be scored in the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing. This spreadsheet is located on the Cyber Readiness share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\2 - CND Directives.* *4. Remediate/Track Progress: If assessor is able to access and execute files without a need to know, all permissions for that folder will need to be reassessed and mitigated by the NCC.*	
	SIPRNet Server Inventory a. NOTE: Authentication servers are defined as those that store user credentials and are essential to the authentication process. Authentication servers include, but are not limited to: Certificate servers, Active Directory, RADIUS, Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System (TACACS) and Linux Network Information Services (NIS). b. The site must also maintain a list of all servers under the organization's direct control. The data registry shall contain a detailed accounting of each server (e.g. owning/administrative unit, location, hostname, hardware, HBSS Global Unique Identifier) and a complete system inventory (e.g. installed software to include product and version.) It must also include all applied patches, STIGs, IAVM, antivirus updates, of any other software updates. c. Note: The data registry must be kept current within 30 days and in a format that can be readily exported to .XLS/.XLMX upon request. The AO shall review	SCOO SCOI

	this registry on a quarterly basis. *This assessment applies to all systems (servers) connected to the local SIPR Network IAW CTO 06-02.* - *Create checklists from STIGs for the following areas: (Windows OS, Internet Explorer Browser, Internet Information Server for Web section, SQL Server Database and Instance for the Database section), IAVMs (Windows Information Assurance and Windows Server Security Technical Guide) and Policy checklists along with STIG viewer from the following website (http://iase.disa.mil/stigs/Pages/index.aspx).*	

16.2. Baseline Scoring and Documentation – CND Directives

16.2.1. Final results of assessment shall be recorded by the WCO on the Cyber Readiness Master Tracker located on the network share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\6. Master Tracker.

16.2.2. Each RAO shall ensure ARSCI is updated to reflect changes as part of assessment closeout procedures on the network share: \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

16.3. Sources

16.3.1. Identify all applicable directives (**https://disa.deps.mil/ext/cop/fs-ccri/inspections/CCRIPAGES/CCRI%20PHASE%20IV.aspx**)

17. Technology Areas

17.1. The Technology Areas are assessed using the DoD mandated STIG via checklists available through the DISA STIG viewer.

17.2. Assessment Procedures (Refer to the table below for your specific area)

17.2.1. Obtain the most recent STIG viewer and the associated STIG according to the Technology Area as assigned from Table 17.1.

17.2.1.1. Note: STIGs and the STIG Viewer are obtained from DISA IASE (**http://www.iase.disa.mil**)

17.2.2. Open STIG Viewer and import STIG to create checklists from STIG selected.

17.2.3. Save as 'STIG Name Checklist mmmyy v#.ckl' Save STIG checklists (.ckl) on the network share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\3 - Technology Areas\Sections in the appropriate folder.

17.2.4. Execute checklists following instructions in the STIG SOP \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

17.2.5. Automated checks are available for certain STIGs such as Operating System and Microsoft Office using SCAP Tools and benchmarks available at DISA IASE (**www.iase.disa.mil**).

17.2.5.1. Note: a quarterly update to the STIG(s) and/or mitigation action will result in a change with the POA&M as well as a change in the score overall. Any change to the POA&M shall require an update to the file version accordingly.

Table 6. STIG Matrix.

Applicable STIGs	Devices Assigned
Database - SCOO	
Database Instance Database STIG Operating System STIG IAVM STIG Browser Microsoft .NET Framework 4.0 STIG	PEX (QKKG-AS-PEX2P) Solarwinds DB (52QKKG-DB-SWNDP) Local SOPs and checklists are found here: Local SOPs and checklists are found here: \\QKKG-FS-022V\SCO\SCOO\2. Configuration\Tab F- Misc\SCAP\Completed Checklists
Web - SCOO	
IIS 7.0 Web Server STIG IIS 7.0 Web Site STIG Operating System STIG Browser STIG IAVM STIG Microsoft .NET Framework 4.0 STIG	ePEX (QKKG-WS-PEX2P) Solarwinds Web (52QKKG-AS-SWNDP Local SOPs and checklists are found here: Local SOPs and checklists are found here: \\QKKG-FS-022V\SCO\SCOO\2. Configuration\Tab F- Misc\SCAP\Completed Checklists
Windows OS (Server) - SCOO | SCOST	
Windows 2008 R2 Member Server STIG Windows 2008 R2 Member Server IAVM STIG McAfee Antivirus STIG (Managed) Microsoft .NET 4.0 STIG Internet Explorer STIG	Backup Server (MIBU01) File Server (QKKG-FS-FIN1P) Print Server (52QKKG-QS-001V) Print Server (52QKKG-QS-003V) Print Server (QKKG-QS-005V) Network Management (52QKKG-NM-01P) Network Management (52QKKG-NM-011V) Network Management (52QKKG-NM-012V) Network Management (QKKG-NM-002P)

Windows OS (Workstation) - SCOO | SCOST	
MS Office System 2013 MS OneNote 2013 MS Lync 2013 Internet Explorer 11 STIG MS Outlook 2013 MS PowerPoint 2013 MS Word 2013 MS Publisher 2013 MS Access 2013 Windows 7 STIG Windows 7 IAVM STIG Microsoft .NET 4.0 STIG McAfee Antivirus STIG (Managed)	Random Workstation (one of each baseline)
Internal Network - SCOI	
Infrastructure L2 Switch (Generic) Infrastructure L2 Switch - Cisco Infrastructure L3 Switch (Generic) Infrastructure L3 Switch - Cisco Infrastructure Router STIG (Generic) Infrastructure Router STIG - Cisco Network Infrastructure Policy STIG IPSEC VPN Gateway STIG Cisco IAVM STIG	EBN Brocade SX EBN Cisco ITB Brocade SX MLS Nexus MDG Core Router Draughon Range VoIP Gateway Router Local SOPs and checklists to assist are found here: \\QKKG-FS-022V\SCO\SCOI\SCOI - NETMAN\03 - Standard Operating Procedures\NETMAN SOPs CR365.
VVoIP and VTC Review - SCOI	
VVoIP STIG VVoIP Policy STIG Video Teleconference STIG Video Teleconference Services Policy VVoIP IAVM CISCO Layer 3 STIG	Cisco IP Phone 7800 Series Cisco IP Phone 7900 Series Cisco IP Phone 8800 Series Cisco IP Phone 9900 Series Cisco IP CIPC Telecore 2151 Call Manager 8.6 (Publisher) Call Manager 8.6 (Subscriber) Cisco Unity Server Local SOPs and checklists are found here: Local SOPs and checklists are found here: \\QKKG-FS-022V\SCO\SCOI\SCOI - Voice.

Site Vulnerability Scan - SCOO	
ACAS scan policy plugins CTO 09-002 Disable Autorun policy Credentialed scan policy	All AFNET workstations Network devices VVoIP and VTC devices PM Systems
Traditional Security – SCQ, FW/IP, ISSM	
Traditional Security STIG	This assessment applies to local personnel security, INFOSEC, physical security, industrial security, COMPUSEC, COMSEC, TEMPEST, and Counter Intelligence. The Wing IP Office should be leveraged to gather the required STIG information. - *Checklist procedures: The inspections include interviews with base personnel, visual inspections, and reviewing physical security practices (administrative and physical):* *1. Base POCs for respective Traditional Security STIG areas are actively involved in the CRP.* *2. Maintain a list of Base Traditional Security POCs.* *3. POA&Ms are initiated and managed by respective POCs.* *4. All STIG updates are relayed to respective POCs.* 5. *A bi-annual review is conducted for Traditional Security accuracy across the base.*

17.3. Baseline Scoring and Documentation Procedures – Technology Areas

17.3.1. Results of the completed STIG checklists from Table 17.1 are recorded onto a local STIG tracker assigned for each Technology Area for scoring located on the network share at \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\1. Checklists\3 - Technology Areas.

17.3.2. These scores are then consolidated and compiled into a Master Tracker by the WCO to produce an overall score across all sections (Contributing Factors, CND Directives, and Technology Areas).

17.3.2.1. Open findings or vulnerabilities discovered during the assessment phase shall be resolved IAW remediation procedures as described in Section 18.

17.3.2.2. Each RAO shall ensure the ARSCI is updated to reflect changes as part of assessment closeout procedures on the network share \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\6. Master Tracker.

18. Remediation Activities (POA&M)

18.1. Vulnerabilities found as a result of running a STIG checklist shall be resolved IAW established vulnerability management processes. Any vulnerability that cannot be resolved immediately shall be managed in a POA&M.

18.2. POA&Ms are created from the STIG checklists using the Vulnerator tool located on the network share \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

18.3. Retrieve the latest version of Vulnerator.

18.4. Import saved STIG checklists (.ckl file) results as described in section 23.2.4 into Vulnerator.

18.4.1. For assistance in using Vulnerator, see how to guide located on network share \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\5. Tools.

18.5. Once all .ckl files are imported click 'EXECUTE' option.

18.6. Upon execution of Vulnerator save as [technology_area POAM-NIPR [SIPR].xls] on the network share \\QKKG-FS-022V\FOUO CCRI_Cyber Readiness\Cyber Readiness\2. POAMs\TECHNOLOGY AREA (i.e. “Internal Network POAM-NIPR.xls”).

18.7. The POAM will be used as a basis for further management and tracking of changes as they occur i.e. (i.e. mitigation activities).

18.8. Once the POA&M is developed, fix actions are prioritized based on impact to the score as documented on the STIG tracker (i.e. develop a priority matrix sorted by CAT I, CAT II, and CAT III findings).

18.9. Quarterly update to the STIG(s) and/or mitigation action will result in a change with the POA&M as well the score overall. Any change to the POA&M shall require an update to the file accordingly.

18.10. At this point, the POA&M is used for the score on the local CCRI Grading Criteria Worksheet and reported as part of the Cyber Readiness Monthly Briefing.

19. Manage Changes

19.1. The responsibility of the below actions falls within scope of mid-level management (i.e. NCO, Supervisor, Section Chief).

19.2. Once a Technology Area has been baselined using STIGs, the completed checklists must be monitored for changes as new STIGs are released on a quarterly basis. .

19.2.1. As new STIGs are released, managers are expected to assist with the following:

19.2.2. Retrieve the latest version of STIGs, IAVMs and STIG viewer from the following website (**http://iase.disa.mil/stigs/Pages/index.aspx**).

19.2.3. When comparing the new STIGs against an existing baseline, focus should be on working the new items introduced with the new STIG.

19.2.3.1. A line-by-line review of the new STIG checklists in comparison to existing POA&M should be accomplished. Checklist items that have not changed do not need to be re-accomplished

19.2.3.1.1. Ensure to copy over notes and pertinent items from the existing POA&M to the new checklist.

19.2.3.2. Upon completion of the comparison, execute assessment procedures on the remaining STIG checks as described in para 17.2.

19.2.3.3. Generate a new POA&M as described in para 18.

R. SCOTT JOBE, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 17-1, *Information Dominance Governance and Management, 12 April 2016*

AFI 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process, 17 Dec 2015.*

AFI 17-130, *Information Assurance (IA) Management* (Superseding AFI 33-200)

AFI 33-324, *The Air Force Information Collections and Reports Management Program, 6 Mar 2013.*

AFMAN 33-363, *Management of Records, 1 Mar 2008*

AFMAN 33-326, *Preparing Official Communications, 25 November 2011*

MPTO 00-33A-1109, *Air Force Information Network (AFIN) Vulnerability Management*

Adopted Forms

AF Form 649, Verification of Long Distance Telephone Calls

AF Form 847, Recommendation for Change of Publication

AF Form 1072, Authorized Long Distance Telephone Calls