***BY ORDER OF THE COMMANDER OF THE 502D AIR BASE WING***

***JOINT BASE SAN ANTONIO INSTRUCTION 17-001***

***7 OCTOBER 2024***

***Cyberspace***

***ENTERPRISE NETWORK SECURITY***

**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: 502 CS/SCXS

Certified by: 502 CS/CC

Pages: 25

---

This publication implements Air Force (AF) Publishing Directive (AFPD) 17-1, *Information Dominance Governance and Management*. It provides guidance and procedures on Joint Base San Antonio (JBSA) Enterprise Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet) throughout JBSA. It applies to all system users and personnel who maintain, administer, and operate the systems, hardware, or software, on the JBSA enclaves. It also applies to the Air Force Reserve and Air National Guard (ANG), except as noted otherwise. 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. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) listed above 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. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, 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 Department of the Air Force.

**1. Overview.** This instruction blends multiple cybersecurity policies necessary to protect mission critical resources (equipment, personnel, data, etc.) from denial-of-service, damage, tampering, espionage, fraud, misappropriation, misuse, unauthorized modification, and unauthorized disclosure. This instruction puts into effect the set of rules and practices that regulate the management, use, protection and distribution, creation, destruction, and manipulation of data entrusted to the JBSA NIPRNet and SIPRNet enclaves.

**2. Roles and Responsibilities.**

2.1. **Joint Base San Antonio Commander.** The JBSA Commander (502 ABW/CC) designates the 502d Communications Squadron Commander (502 CS/CC) as the Wing Cybersecurity Officer to address all cybersecurity and mission critical resources to ensure operational integrity is maintained throughout the life cycle of resources and security of JBSA NIPRNet and SIPRNet enclaves.

2.2. **502 CS/CC.**

2.2.1. Appoints a Wing Information System Security Manager (ISSM).

2.2.2. Will function as the JBSA NIPRNet and SIPRNet enclave Information System Owner (ISO) and Program Manager (PM).

2.2.3. Ensures proper procedures are in place to maintain information systems to operate effectively and securely.

2.3. **The Wing Cybersecurity Officer.**

2.3.1. Evaluates modifications, exceptions, and deviations to JBSA information systems.

2.3.2. Ensures system and network compliance with Higher Headquarters instructions and manuals.

2.3.3. Ensures periodic health check scans and quarantine and/or removal of systems (servers, workstations, laptops, printers, and other miscellaneous network devices) from the network that exceed cybersecurity vulnerability established thresholds.

2.4. **JBSA Information System Security Manager (ISSM).**

2.4.1. Responsible for the JBSA NIPRNet and SIPRNet cybersecurity programs that connect to the Air Force Information Network (AFIN) and has the authority, in collaboration with the 502 CS/CC (Wing Cybersecurity Officer) to create and enforce more stringent local policies and procedures for the JBSA NIPRNet and JBSA SIPRNet enclaves.

2.4.2. Evaluates documented vulnerabilities and risks that affect the JBSA enclaves and makes risk determinations, in coordination with the Wing Cybersecurity Officer, on any action that would elevate the network risk.

2.5. **User Responsibilities.** There are users for different systems and networks with responsibilities outlined below for each type of system or network.

2.5.1. All network users will sign an DAF Form 4394, *Department Of The Air Force User Agreement Statement - Notice and Consent Provision,* a Rules of Behavior and Acceptable Use Standards for Information Technology (See **attachment 2**), and complete current Department of Defense (DoD) Cyber Awareness Challenge training prior to gaining access to the AFIN. Users utilizing mobile devices as identified in AFMAN 17-1301, *Computer Security (COMPUSEC),* to include but not limited to smartphones, tablets, and laptops, will be required to sign the DAF Form 4433, *The Department of the Air Force Mobile Device User Agreement*. The DD Form 2875, *System Authorization Access Request (SAAR),* is no longer mandatory for an unclassified user account on the AFIN to be provisioned. However, the DD Form 2875 will be utilized to document network access after provisioning and for access to systems, folders, groups, security groups, share drives, organizational mailboxes, applications, and any other accesses owned by the unit.

2.5.2. All JBSA Privileged Users utilizing a role-based administrator account, such as Workstation (.ADW) or Functional Server (.ADF) admin accounts, will remain in compliance with DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program,* and DAFMAN 17-1305, DAF *Cybersecurity Workforce Management Program,* policies and regulation, with regards to certification, training, and position requirements.

2.5.3. NIPRNet users must log in using a DoD issued Common Access Card (CAC) with a 16-digit Personal Identity Verification certificate. A digital signature is required for all official email correspondence sent from a DoD-owned, operated, or controlled system or account to include desktops, laptops, tablets, and personal electronic devices such as iPads and mobile phones. E-mails which contain Personally Identifiable Information (PII) such as a Social Security Number or Controlled Unclassified Information (CUI) must be properly marked, encrypted, and digitally signed to reduce the risk of compromise.

2.5.4. SIPRNet users must log in with a Public Key Infrastructure (PKI) token card unless they are on a Defense Information Systems Agency (DISA) approved disadvantaged user list.

2.6. **Unit Information System Security Officer (ISSO) Responsibilities.**

2.6.1. Each unit must have a primary and an alternate ISSO appointed in writing by the unit Commander or Director. The approval for ISSO appointment cannot be delegated to a lower level unless the Commander or Director is absent. In that instance, the Deputy Commander or Deputy Director may sign. This appointment letter will be updated on an annual basis, when appointed ISSO personnel change, or when a new Commander takes command. An updated copy must be provided to the JBSA Wing Cybersecurity Office (WCO).

2.6.2. The unit ISSO is the sole contact between the unit and the JBSA WCO on all cybersecurity matters.

2.6.3. The unit ISSO is responsible for implementation of the cybersecurity program at the unit level, based on JBSA WCO policies and guidance, and ensures compliance with AFI 17-101, AFI 17-130, DAFMAN 17-1301, DAFMAN 17-1304, DAFMAN 17-1305, and

applicable cybersecurity DoD Instructions, Manuals, and National Institute of Standards and Technology guidance.

2.6.4. It is the responsibility of the unit ISSO, Information Assurance Officer (IAO), Cybersecurity Liaison (CL), or Commander's Support Staff (CSS) to maintain and track user documentation as identified in **paragraph 2.5** throughout the lifecycle while the individual is assigned to JBSA Lackland or JBSA Randolph, including Chapman Annex and Port San Antonio. The all-inclusive reference of unit ISSO will be used from this point forward to describe unit cybersecurity duties. This documentation must be maintained by the unit ISSO on Electronic Records Management (ERM) folders, organized in a standard format, and readily available upon request from the 502 CS and Higher Headquarters.

2.6.5. Unit ISSOs will collect all documentation required for privileged access, to include unit appointment letter, DD Form 2875 for each role, copy of Computing Technology Industry Association (CompTIA) or equivalent certifications, signed Privileged User Agreement, signed Formal Statement to validate position/contract requirements, validate position is properly coded in the Unit Manning Document (UMD), and Privileged User Cybersecurity Responsibility training certificate. Unit ISSOs will work with the JBSA WCO and will follow the procedures for account creation, as presented by the 688 CW/A6, Enterprise Access Management Organization.

2.6.5.1. The unit ISSO is responsible to complete a quarterly and upon request, audit, and validation of privileged users documentation identified using the JBSA NIPR Privileged User Account Tracker (available on the JBSA WCO SharePoint site at **https://usaf.dps.mil/sites/aetc-jbsa-cs/scx1/ia/sitepages/compusec.aspx**) for NIPRNet and SIPRNet. This audit will be utilized to determine that privileged users have a continuing requirement for privileged capabilities or access and to help meet Cyber Operational Readiness Assessment (CORA) (formerly Command Cyber Readiness Inspection (CCRI)) requirements. When ISSO completes the audit, they will submit the documentation through their unit personnel security office for validation of the privileged user's security clearance is still active and current.

2.6.5.2. When the entire package is complete the ISSO will submit to the JBSA WCO prior to suspense date. If responses for validation of privileged users is not returned within requested timelines, then privileged account will be disabled until proper validation is received.

2.6.6. The ISSO will continually evaluate the need for shared privileged local accounts, restrict for emergency use only, document, and continuously monitor for unauthorized activity.

2.6.7. The ISSO will ensure that the most current version of the JBSASANANTONIOVA17-1301, *Joint Base San Antonio (JBSA) Cyberspace Protection Condition (CPCON)* visual aid is downloaded from the AF E-Publishing website or the COMPUSEC HUB. The proper use of this document must be briefed to all unit personnel and displayed within eyesight of any AFIN connected device. Additionally, users need to be aware of the current CPCON and know that the CPCON level is located on their display monitor in the top left corner of the green banner header.

**3. Use of Unapproved Media.**

3.1. **Flash Memory Devices.** The use of flash memory devices (i.e., thumb drive, memory cards, cell phones, cameras, PDAs, MP3 players, e-readers, tablets, etc.) is prohibited on government furnished equipment (laptops/tablets) on and off the network.

3.2. The Air Force implemented the Microsoft Defender Endpoint® (MDE), a unified program management suite that uses client agents to prevent, track, report, and remediate malicious computer related activities and incidents.

3.2.1. The data loss prevention component blocks unapproved universal serial bus (USB) devices from attaching to computer systems on DoD networks. The use of these devices will result in immediate network account suspension.

3.2.2. Reinstatement of Network Access. To reinstate network access, the user must re-accomplish DoD Cyber Awareness Challenge training and provide a copy of the training certificate along with a Network Access Reinstatement Request and Letter of Assurance signed by the individual's commander or two-letter directorate chief to the 502 CS/SCXS, JBSA Wing Cybersecurity ISSM.

**4. JBSA Network Enclaves.**

4.1. **Separate Network Enclaves.** The JBSA NIPRNet and SIPRNet are separate network enclaves. Users must maintain separate equipment for each network. No physical connections are authorized between NIPRNet and SIPRNet.

4.1.1. No media will be transferred between NIPRNet and SIPRNet without approval from the AF Authorizing Official (AO) and consideration of an official Cross Domain Solution first ( **https://usaf.dps.mil/teams/ccc/fpu/Air-Force-Cross-Domain-Support-Element.aspx** ).

4.1.2. Any unclassified media placed into a SIPRNet system becomes classified and must be safeguarded or destroyed in accordance with applicable classification guidance.

4.2. **Program Management Office (PMO) Systems.**

4.2.1. Any system that has its own Authorization To Operate (ATO), performs unique patching, and uses IP space provided by the JBSA NIPRNet or SIPRNet circuits is considered a PMO system.

4.2.2. All PMO systems are required to be identified to the WCO for CORA awareness, including the following information: IP addresses, PMO information, ISSM/ISSO information, system description, and provide a copy of the current ATO (and updates in ATO status).

4.2.3. PMO systems are required to meet all NIST, DoD, and AF guidance, as well as, JFHQ-Department of Defense Information Network (DODIN) CORA/CCRI Process Guides/OI's/Checklists: Supply Chain Risk Management Process, Cybersecurity and Resiliency Process Guide (includes System of Record of Notices, Privacy Impact Assessments, and Cloud Provisional Authorizations), Endpoint Security Process Guide, Cyber Defense – Monitor, Detect, and Respond Process Guide (includes Cyber Security Service Provider (CSSP) alignment), Insider Threat Process Guide, and Key Indicator of Risk Guide.

4.2.4. PMO will notify and provide documentation to the WCO immediately if a PM system, server, or application is decommissioned. PMO systems are required to abide by all GENADMINs distributed by the 502 CS. If unable to comply, then PMO systems are required to submit a Plan of Actions and Milestones (POA&M) that includes timelines and milestones to be in compliance.

4.3. **Systems, Networks, and Internet Service Providers (ISP).** Organizations will not install government owned or funded wired or wireless systems/networks or use government funded Commercial ISP (C-ISP) without a completed Cyberspace Infrastructure Planning System (CIPS) ticket. All C-ISP must have an Authorization To Operate (ATO), must be registered in the DISA SNAP database (if possible) before operation (See **https://usaf.dps.mil/sites/13057/Office-of-the-CISO/CNZP/SitePages/CISP.aspx** ), and abide by the Network Infrastructure Policy Security Technical Implementation Guide. Any unauthorized systems, networks, wireless access points, or C-ISP connections will be disabled, disconnected, and/or turned off immediately upon discovery until an ATO and/or Approval to Connect (ATC) as well as an approved non-Defense Information Systems Network (DISN) waiver (**https://usaf.dps.mil/teams/EAO/Pages/CISPWiki.aspx** ) is obtained. The only exception is for an ISP connection to a non-DoD network (such as a contractor-owned infrastructure) co-located on the same premises as the DoD network. The non-DoD network is physically and logically separated from any DoD IP network. Furthermore, it is not connected to any DoD IP network. The non-DoD network infrastructure is not DoD funded nor is it operated or administered by DoD military or civilian personnel. In addition, the non-DoD network with the ISP connection is not storing, processing, or transmitting any DoD data. For such a network as defined herein, a DoDIN Waiver approval is not required for deploying a connection to an ISP. However, the AO must perform and have on file a risk assessment endorsed by the facility or installation command. For guidance on unique situations, contact the JBSA WCO.

4.4. **Standalone Systems.** Standalone systems must be authorized through one of three processes by the unit ISSO. All documentation must be maintained by the unit ISSO and provided to the JBSA WCO, and upon request by appropriate parties, to provide evidence of authorization. If the standalone is:

4.4.1. A Standard Desktop Configuration and STIG compliant single system, then document security control compliance, submit results to the enclave ISSM for review, and if approved, obtain a Standalone System Authorization Memorandum or No Security Impact Memorandum.

4.4.2. A kiosk, then complete appropriate kiosk Risk Management Framework (RMF) guidance at

https://usaf.dps.mil/sites/aetc-hq-a6/A6C/A6CR/SitePages/Kiosk-Guidance.aspx.

4.4.3. All other situations, then document applicable security control compliance by completing the RMF process and registering the system in the Enterprise Mission Assurance Support Service (eMASS) at **https://airforce.emass.apps.mil/**.

4.5. **End of Life/End of Support.** Devices and software on the network must be patched/remediated and kept up to date with the most current approved versions of firmware, software, and hardware that is available from vendors to ensure adequate countermeasures are applied across the AFIN**.** Legacy versions of firmware, software, and hardware are not authorized on the AFIN. Failure to maintain proper versions and support for firmware, software, and hardware will result in removal from the AFIN. This will ensure STIG compliance and vulnerability management is adhered to on the JBSA segment of the AFIN. To maintain compliance and replace legacy equipment/software it is the organizations responsibility to budget and replace or upgrade any devices, operating systems, and software prior to the equipment/software reaching end-of-life or end-of-support from vendor.

**5. Software.**

5.1. **Software Approvals** . All software running on the network must be part of the authorized Standard Desktop Configuration (SDC) or included on the Air Force Evaluated Products Listing (AF EPL), National Information Assurance Partnership, Common Criteria, or Approved Products List Integrated Tracking System**.** All software certifications must include a security risk assessment that includes vulnerabilities and mitigations for the software. Software certifications on the listings above are for specific versions and expire on specific dates. Before the old version expires, it is the unit ISSO's responsibility to submit the paperwork necessary to get the software recertified (normally one year in advance of expiration). New major versions of the software must also be submitted for certification before usage.

5.1.1. Reciprocity for software from other certifying agencies is not an automatically approved process. The requestor must ensure that the certification document contains any security vulnerability findings and remediation actions. If the software contains a Category 1 (Very High or High risk) finding that cannot be remediated the request will be disapproved. If a Category 1 finding is identified at a later date that cannot be remediated the software must be immediately removed from the enclave.

5.1.1.1. The user must submit a completed Application Request Worksheet (ARW) located on the following website for all software not on the AF Evaluated Products Listing (AF EPL): **https://usaf.dps.mil/teams/ccc/fpu/CZZE_TE_SACA.aspx** . The ARW will be attached to the Cyberspace Infrastructure Planning System (CIPS) request document for validation/review by the WCO. Once the CIPS requirement is approved the requestor must submit the ARW to the HQ CCCC/SACS Software Certification Assessments for testing. Additional information can be located on the link in **paragraph 5.1.1.1**.

5.1.1.2. The JBSA ISSM is the ultimate authority for acceptance/non-acceptance of vulnerabilities and risks created using software on all JBSA NIPRNet and SIPRNet enclaves. The ISSM may delegate this authority to the WCO staff.

5.1.2. At no time will personally owned or personally developed software be used on the JBSA enclaves.

5.1.3. All non-SDC software or Software as a Service (SaaS) must be tested, vetted for use, and have a current certification memorandum prior to being added to the enclave. This requires an approved CIPS request prior to loading on to any JBSA enclave.

5.2. **Upgrades and New Software Versions.**

5.2.1. Prior to purchasing upgrades and/or new versions of software, Unit Software License Managers (USLMs) in coordination with their ISSO must submit a new CIPS work order to ensure approval is authorized.

5.2.2. All software must be installed and maintained in accordance with all applicable DISA Security Technical Implementation Guides (STIGs), and all stipulations and conditions identified in the approval documentation must be enforced by the unit ISSO. Software with un-remediated vulnerabilities will not be allowed on the network. At no time will software with a Category 1 vulnerability that cannot be remediated be allowed on the NIPRNet/SIPRNet enclaves. Failure to abide by the conditions of the approval will result in the removal of the software until the conditions can be properly met.

5.2.3. Unit ISSOs, Functional System Administrators (FSAs), and Client Systems Technicians (CSTs) must ensure all network and standalone device's/system's software remains compliant, including with all issued GENADMINss. All USLMs must ensure that proper licenses are in place for software running on computers in their organizations. USLMs must work with the Base Software License Manager to ensure their unit licensing program is compliant with current AF requirements.

5.2.4. USLM will submit an annual inventory of software, version, number of licenses, and approval memorandum to the Base Software License Manager (BSLM).

5.2.5. When unauthorized software is identified, the BSLM will coordinate the removal of the software with the USLM and the ISSO for that specific unit.

5.3. **Software Development and Coding.**

5.3.1. All software application development and coding must be performed in an approved development environment that is not connected to the AFIN. All development and code using programming languages and tools (i.e., Python, JavaScript, Java, C++, R, PHP, Swift, Go, PERP, etc.) must have a code analysis and vulnerability assessment completed that demonstrates there are no Critical or High vulnerabilities before being introduced into a production environment.

5.3.2. The software and code must be tested before each version release and annually for programming vulnerabilities and functional exploits to maintain a secure software baseline. Personnel who perform software development, programming, engineering, or coding must meet the unique certification requirements as dictated in DoDM 8140.03 and DAFMAN 17-1305.

5.3.3. All testing of new hardware, software, configurations, or applications must be performed on an approved test bed or test environment that is not connected to the AFIN.

5.4. **Reboot of Computers.** All computers will automatically reboot after 72 hours of uptime. A user can prevent interruption of work and loss of data by restarting the computer instead of shutting down at the end of each duty day. Teleworkers must ensure their laptop/workstation stays connected to the Virtual Private Network (VPN) in order to receive software patches/updates and to avoid quarantine. At the end of the day simply remove your CAC – DO NOT disconnect/DO NOT log off/DO NOT restart/DO NOT shut down your system.

**6. Scanning.**

6.1. The 502 CS Vulnerability Assessment Technicians (VATs) have established a JBSA Scan Battle Rhythm Calendar (SBRC) outlining the overall scan process which is published annually to all mission partners. VATs will perform weekly vulnerability scans of the JBSA Randolph and Lackland NIPRNet and SIPRNet enclaves. Scanning is conducted using DISA or AF approved scanners, tools and software operated by the 502 CS. Units are responsible for ensuring all NIPRNet/SIPRNet systems are online and scanned weekly per USCYBERCOM TASKORD 20-0020. VATS will use scan data to identify systems which pose the greatest risk to the enclave for removal from the network. Scans needed outside of the SBRC will require a formal request via the current trouble ticket reporting mechanism for VATs to validate corrective actions**.**

6.1.1. Systems identified as a risk to the enclave based on scan data with a 30-day filter applied on NIPRNet or SIPRNet enclaves will have the following actions executed:

6.1.1.1. Systems will be identified as Over Threshold Limit (OTL) and identified to unit CSTs monthly via GENADMIN. OTL systems will also receive a pop-up notification directing the user to contact their unit CST or FSA to remediate the system's vulnerabilities.

6.1.1.2. Systems will be re-scanned IAW established SBRC re-scan dates to establish the Targeted Removal Listing (TRL) which will be sent to CSTs or FSAs monthly via GENADMIN.

6.1.1.3. All TRL systems will be quarantined from the network and require a formal request via the current trouble ticket reporting mechanism by VATs to validate corrective actions and be removed from quarantine.

6.1.1.4. As per TO 00-33A-1109 para 7.10.1.1 once quarantined, a system must be remediated to acceptable network standards before being removed from quarantine and restored to full network access.

6.1.1.5. Any system that remains a risk to the enclave and quarantined by the next SBRC monthly quarantine cycle will be removed from the network.

6.1.2. Per TASKORD 20-0020 3.C.1.B. Local systems administrators must ensure appropriate authentication access and credentials are provided to Base VATs. The following actions will be taken on Bad Access/unavailable systems:

6.1.2.1. Systems identified as Bad Access or reported as "Unknown" will require restoral of access within 14 calendar days. If not corrected, the system will be removed from the network. **Note**: Some systems may require a re-image to apply necessary security settings.

6.1.2.2. System owner will submit a formal request via the current trouble ticket reporting mechanism for validation of credentialed access by Base VATs. Once validated, system will be removed from the pop-up notification.

6.1.2.3. Systems that are not remediated within identified remediation period will be submitted for quarantine.

6.1.2.4. Once quarantined, credentialed access must be validated by VATs before being removed from quarantine and restored to full network access.

6.1.2.5. Any system that remains without credentialed access and quarantined by the next SBRC monthly quarantine cycle will be removed from the network.

6.1.3. The 502 CS will perform periodic targeted STIG compliance scans of all JBSA network assets (clients, servers, workstations, laptops, printers, and other miscellaneous network devices) and provide results to the JBSA Wing Cybersecurity Office as required for ATOs. Failure to meet DISA STIG compliance could result in removal of network access. NOTE: Higher Headquarters actively quarantines based on their own criteria . The 502 CS has no authority to manage quarantine actions initiated by other Air Force entities.

**7. Periodic Health Checks of Systems and Networks.**

7.1. The 502 CS will perform periodic health check scans and quarantine and/or remove systems (servers, workstations, laptops, printers, and other miscellaneous network devices) from the network that exceed cybersecurity vulnerability thresholds established by DISA, USCYBERCOM, the JBSA Information Security Officer, or if they meet one or more of the following criteria:

7.1.1. Systems without Microsoft Endpoint Configuration Manager® (MECM) client installed or misconfigured.

7.1.2. Systems without the Trellix/MDE client installed or misconfigured.

7.1.3. Systems without TANIUM client installed or misconfigured.

7.1.4. Program Managed Office systems with a CAT 1 finding and no approved Plan Of Action & Milestones (POA&M).

7.1.5. Inoperable anti-virus client and/or modules.

7.1.6. SIPRNet systems with a wireless network card installed.

7.1.7. Systems not in compliance with the established naming convention.

7.1.8. SIPRNet systems that missed two consecutive vulnerability scans. NOTE: The ISSM/AO may change the disconnection criteria as needed to protect the Air Force network and JBSA's mission.

**8. Manual Remediation and Patching.**

8.1. New systems, systems excluded from automated remediation, or off-line (standalone) systems must be configured to meet DISA STIG and/or the Security Content Automation Protocol tool requirements. The assigned unit ISSO, FSA, or CST will document all exemptions or risks accepted by the AO via an AF Form 4169, *Request For Waiver From Waiver Information Assurance Criteria* or POA&M.

8.2. As JBSA Information Security Officer, the 502 CS/CC may disconnect any system which presents a serious risk to the network until fully compliant and remediation is validated by 502 CS.

8.3. Servers and systems utilizing service accounts are required to ensure compliance with the latest version of Maintenance Task Order (MTO) 2020-069-001x. Service account password changes must be accomplished at minimum every 365 days and meet the password complexity, as per the operating system STIG.

**9. Task Orders (TASKORD), Notices to Airmen Message (NOTAMs), Cyber Tasking Orders (CTO), and STIGs.**

9.1. The 502 CS receives and disseminates all TASKORD, NOTAMs, CTOs, and STIGs. 502 CS determines applicability for JBSA organizations and establishes suspense dates. Network compliance orders and directives carry the weight of higher agency orders and protect and assure availability of the network and are equivalent to Air Tasking Orders in the cyber warfare domain. They are a vital component in our ability to "Fly, Fight, and Win…Airpower Anytime, Anywhere."

9.2. Organizations will comply with all published network compliance orders and directives on or before mandatory suspense dates.

**10. Network Infrastructure, Media Access Control (MAC), MAC Authentication Bypass (MAB) and Port Security.**

10.1. MAB and/or port security will be configured on all network switch ports across JBSA. Ensuring only authorized devices are connected to the network is fundamental to maintaining network security. JBSA utilizes 802.1X-M.

10.2. An Enterprise Service Desk (ESD) trouble ticket must be submitted to the Communications Focal Point (CFP) to add the network device's MAC address to the MAB database. After the MAC address is added to the database, the network device can be plugged into any active port, and it will be authenticated and allowed to connect to the rest of the network.

10.3. JBSA-Lackland and JBSA-Randolph maintain their own MAB databases. Users traveling across JBSA must request addition to both databases on the ESD trouble ticket submission. Requests to temporarily disable port security must be approved by 502 CS/CC for NIPRNet and SIPRNet.

10.4. If a request for a MAC to MAB is for an Advanced Battle Management System (ABMS) DeviceOne SecureView (ADSV) in-garrison workstation, then the requester is required to notify the JBSA Wing Cybersecurity Office before operations occur, including IP addresses used to the group e-mail box: **502cs.ia@us.af.mil**.

**11. Network Infrastructure, 802.1X Comply-to-Connect (C2C) Zero Trust, Port Security Media Access Control (MAC), MAC Authentication Bypass (MAB).**

11.1. **802 1X will be configured on all network switch ports across JBSA.** Connected end devices such as PCs, telephones, and printers will use certificates. MAB will be used for devices that are not able to use certificates to authenticate to the network. Ensuring only authorized devices are connected to the network is fundamental to ensuring a baseline network security posture. JBSA utilizes 802.1X per DISA STIGs and JFHQ DODIN TASKORD 21-0024 C2C.

11.2. An Enterprise Service Desk (ESD) trouble ticket must be submitted to the Communications Focal Point (CFP) to add the network device's MAC address to the MAB database. Once MAC address is added to MAB, the device can be plugged into any active port, and it will be authenticated and allowed to connect to the network.

11.3. JBSA-Lackland and JBSA-Randolph utilizes C2C appliance for implementation. Users traveling across JBSA will be able to connect to active ports without an ESD ticket for each location. The C2C appliances uses the same database across all AETC bases.

**12. DoDM 8140.03 Certification Requirement.**

12.1. All personnel (military, civilian, and contractors) occupying a cybersecurity workforce position must be coded with a DoD Cyberspace Workforce Framework (DCWF) code and complete applicable DoDM 8140.03 workforce qualification education, training, and commercial certification requirements. Personnel must release certification information to the Cyberspace Workforce Improvement Program: **https://cwip.cce.af.mil/IAWIP/CyberSecurity.cfm**.

12.2. Personnel with admin accounts will maintain appropriate sensitivity levels, Security Access Requirement (SAR) codes, and certifications IAW DoD Manual 5200.02, *Procedures for the DoD Personnel Security Program (PSP)*, DoDMAN5200.02_DAFMAN16-1405, *Air Force Personnel Security Program*, and DAFMAN 17-1305.

12.3. All cybersecurity workforce positions must be coded properly in both military and civilian personnel systems and written into the contractor's Statement of Work (SOW)/Performance Work Statement (PWS). Contractors must be qualified in accordance with DoDM 8140.03 at the commencement of work.

12.4. All DoDM 8140.03 qualification education, training, commercial certifications, all manning position, or billet data, DCWF codes, privileged user statement, and national security investigation status are to be tracked and maintained by the unit ISSO in accordance with DAFMAN 17-1305 and DAFMAN 17-1301. The unit ISSO will report these statistics to the JBSA Wing Cybersecurity Office annually, and upon request.

**13. Negligent Discharge of Classified Information (NDCI).**

13.1. AFCYBER TASKORD 22-2022 *Negligent Discharge of Classified Information (NDCI) Handling Procedure* stipulates seven procedures: Identification, Declaration, Notification/Tracking, Containment, Sanitization, Incident Party Unlock Procedures, and Account Restoral & NDCI Closure.

13.2. Key players in the NDCI procedures are the unit (leadership, Unit Security Manager, Unit ISSO, CST, CSS) who identified the NDCI, the unit's Information Protection Office, AFIN Mission Assurance Center (AMAC), and the 502 CS.

13.3. Sanitization procedure of any NDCI event will be worked through unit commanders and unit ISSOs. Software used for sanitization must be approved and IAW AF Enterprise Authorizing Official.

**14. Network Security Incidents.** There is zero tolerance for network security incidents. An immediate response by all affected agencies is required to minimize the spread of the virus or malware. Actions will include immediate cessation of all operations on the affected systems, data collection and security measures as warranted by the incident. Remediation of all network security incidents will be worked through unit commanders and unit ISSOs.

**15. Communication Rooms, Closets, and Manholes.** Control of communication rooms, closets, and manholes is imperative to physical network security. All must be locked or secured to protect equipment from intrusion and compromise.

15.1. Access to communications closets will be restricted to 502 CS personnel only. They must be kept clean and properly maintained to ensure the safety of technicians who work in them. Adequate space is required for ladders and tools for technicians to complete tasks.

15.2. Communication rooms and closets are not to be used for storage, breakrooms, or snack bars.

**16. External USB Hard Drives.**

16.1. External USB hard drives must be government procured and owned. Either hard disk drives with New Technology File System (NTFS) formatted or Solid-State Drives (SSD) are allowed and must be properly labeled. All USB external hard drives must be approved and documented in the Data Loss Prevention (DLP) Whitelist Database. Unit ISSOs are trained by the JBSA Wing Cybersecurity Office on their responsibility to process, maintain, update, and track all the required material to ensure there is no disruption to the user. The unit ISSOs will follow procedures outlined in the latest NIPRNet DLP Waiver Spreadsheet MTO 2022-270-002 and MTO 2022-270-003 (MTO to have the external hard drive approved and added to the DLP Whitelist Database).

16.2. Encryption for data at-rest, in-motion, and in-use. Encrypt sensitive information (e.g., Controlled Unclassified Information, For Official Use Only, Personally Identifiable Information, Health Insurance Portability and Accountability Act, Privacy Act, and Proprietary). Validate information assurance/information assurance-enabled products providing encryption according to DoDI 8500.01. CJCSI 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND*) extensively references the DoD CIO Memo "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media."

16.2.1. Use Common Criteria-validated products or National Institute of Standards and Technology (NIST) evaluated cryptographic modules that provide the minimum Federal Information Processing Standards validated cryptographic module implementing Secure Hash Algorithm-256 for data at rest.

16.3. All SIPRNet external USB hard drives must receive authorization via the SIPRNet DLP Exemptions and Burn Rights Process.

## 17. Removable Media.

17.1. Users of removable media will be authorized in writing by their commander or director.

17.1.1. Authorized users of removable media on SIPRNet will undergo initial and annual training. Once completed the user will annually acknowledge in a written agreement their understanding and responsibilities (See **https://intelshare.intelink.sgov.gov/sites/jbs-wco/_layouts/15/start.aspx#/SitePages/COMPUSEC.aspx** for training and user agreement):

17.1.2. Suspected misuse or compromise of removable media is immediately reported to the ISSO, security assistant, and commander.

17.1.3. All removable media will be scanned for malicious code prior to use on any IT asset.

17.1.4. An official will be designated in writing for controlling removable media on SIPRNet through the media's lifecycle. This is a "cradle to grave" process. The designated official will be able to provide process and procedures to assist with validating Insider Threat mitigations.

17.1.5. ISSO will periodically review removable media logs on SIPRNet to ensure they reflect an up-to-date status for all media that is currently being stored.

17.1.6. The data that is removed from any IT system will be properly labeled, safeguarded, stored, destroyed, and disposed of in accordance with the data they contain.

17.2. All removable media is clearly labeled with classification, creator, last modified time, and last modified user. This requirement applies to NIPRNet, SIPRNet, and non-connected or low-bandwidth environments.

17.3. Media must be write-protected on SIPRNet.

17.4. All removable media must be procured in accordance with Air Force approve purchasing guidelines and through mandatory sources.

17.5. All devices must be government owned.

17.6. Removable Media is authorized for use and removable media data will be encrypted, logged, and audited IAW CNSSD 504 Annex A, *Directive on Protecting National Security Systems from Insider Threat*, CNSSP 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems (NSS)*, and DAFMAN 17-1301 guidance.

17.7. All removable media is encrypted (data at rest) users must verify they are utilizing current Federal Information Processing Standard (FIPS) for encryption on all removable media (i.e., BitLocker).

17.8. Use of Cross Domain Solution will be considered in lieu of removable media.

**18. NIPRNet Wireless Devices.** All NIPRNet wireless devices must have an approved 502 CS technical solution (e.g., an approved communications requirement technical solution documented in CIPS Work Order Management System) and be acquired in accordance with DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability*. All wireless devices must abide by DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid*, DAFMAN 17-1301, all applicable DISA STIGs, TEMPEST separation requirements, and meet all FIPS 104-3 requirements. Commercial Internet Service Provider (C-ISP) to include commercial mobile Wi-Fi (Mi-fi) hotpots using cellphone infrastructure must follow the same authorization process as traditional hard wired commercial infrastructure using AFMAN 17-2101 *Long-Haul Communications Management*.

**19. Foreign Nationals.** All foreign nationals (nonresident aliens) who require government information system access are required to have a Foreign Disclosure Package processed by the unit ISSO and approved through the Foreign Disclosure Office and JBSA WCO before access is granted.

**20. Cyber Readiness (CR) 365 Assessments.**

20.1. The JBSA CR 365 assessments provide an extensive CR 365 sight picture using CORA, Department of Defense, Air Force publications and guidance to identify deficiencies in cyber programs and report deficiencies to the organization and Communications Squadron leadership.

20.2. Battle Rhythm:

20.2.1. Unit ISSO's will complete an annual self-assessment of their cybersecurity posture and return to the JBSA WCO NLT 1 October of each year using the latest criteria posted on the JBSA WCO SharePoint site at **https://usaf.dps.mil/sites/aetc-jbsa-cs/scx1/ia/sitepages/compusec.aspx** .

20.2.1.1. Review and report compliance on audit logs of network devices, PowerShell, operating systems of workstations and servers, Intrusion Detection Systems (Boundary/Internal), web, databases, and Cross Domain Solutions. At minimum logs must be reviewed weekly for system health, maintenance, and/or anomalous activity. Internal logs will be forwarded to centralized log server.

20.2.2. The JBSA WCO will conduct, at a minimum, an in-person CR 365 assessment of 10 percent of the JBSA organizations annually. These assessments may be scheduled in advance or may be no-notice assessments. During the assessment, the JBSA WCO team will validate self-assessment documentation, perform a physical walk-through of the organization, interview unit ISSOs, a sampling of users and privileged users within the organization's purview, review Risk Management Framework documentation, and validate compliance with CORA, DoD, and AF guidance.

20.2.2.1. After action reports will be provided to the assessed unit Commander/Director and may be provided to the 502 CS/CC.

20.2.2.2. Deficiencies identified during the assessment must be addressed in writing every 30 days by the unit Commander/Director until resolution of the deficiency is approved by the JBSA WCO.

20.2.3. Organizations may request a CR 365 Staff Assistance Visit (SAV) from the JBSA WCO via official e-mail to **502cs.ia@us.af.mil**. Requests will be completed based on mission and personnel availability within the JBSA WCO.

**21. JBSA NIPRNet and SIPRNet Cybersecurity Programs.** The JBSA ISSM is ultimately responsible for the JBSA NIPRNet and SIPRNet cybersecurity posture and has the authority to create and enforce more stringent local policies and procedures. In the event there are conflicts in the interpretation of cybersecurity policy, the JBSA ISSM is the final authority for the direction and/or actions to be taken.

**22. Network Security** . Network security is the responsibility of everyone. A risk accepted by one user is a risk assumed by all. To this end, it is imperative that all personnel and organizations adhere to AF and DoD security policy and follow this instruction as we continue to improve our network security and make the cyber domain a safer place to perform our mission.

**23. Contacts** . Contact the JBSA Wing Cybersecurity Office, 502 CS/SCXS-Randolph at DSN 487-4231, 502 CS/SCXS-Lackland at DSN 473-8960, or via email at **502CS.IA@us.af.mil** for any questions or concerns.

RANDY P. OAKLAND, Brigadier General, USAF
Commander

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

CJCSI 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND*), February 9, 2011

DODM 5200.02, Procedures for the DoD Personnel Security Program (PSP), 3 April 2017

DoDMAN5200.02_DAFMAN16-1405, *Air Force Personnel Security Program,* 1 August 2018

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid, April 23, 2007*

DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program,* 15 February 2023

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

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 6 February 2020

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

AFI 17-203, *Cyber Incident Handling,* 16 March 2017

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

DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability,* 13 September 2022

AFMAN 17-2101, *Long-Haul Communications Management*, 22 May 2018

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

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

DAFMAN 17-1305, DAF *Cybersecurity Workforce Management Program*, 7 June 2024

JBSASANANTONIOVA17-1301, *Joint Base San Antonio (JBSA) CPCON*, 11 July 2023

CNSSD 504 Annex A, *Directive on Protecting National Security Systems from Insider Threat*, September 2021

CNSSP 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems (NSS)*, July 22, 2021

MPTO 00-33A-1109, *Air Force Information Network (AFIN) Vulnerability Management,* August 1, 2022

MPTO 00-33A-1202, *Air Force Network Account Management,* September 10, 2020

MTO 2020-069-001K, *Active Directory (AD) Object Management*, October 20, 2022

MTO-2022-270-002, *Annual Revalidation of NIPRNet Data Loss Prevention (DLP) Exemptions Process,* October 4, 2022

MTO-2022-270-003, *Annual Revalidation of SIPRNet Data Loss Prevention (DLP) Exemptions Process,* October 4, 2022

USCYBERCOM TASKORD 20-0020, *Assured Compliance Assessment Solution (ASCAS) Operational Guidance,* September 20, 2021

AFCYBER TASKORD 22-2022 *Negligent Discharge of Classified Information (NDCI) Handling Procedure,* January 20, 2023

***Prescribed Forms***

None

***Adopted Forms***

AF Form 4169, *Request For Waiver From Information Assurance Criteria*

DAF Form 4394, *Department Of The Air Force User Agreement Statement - Notice and Consent Provision*

DAF Form 4433, *The Department of the Air Force Mobile Device User Agreement*

DD Form 2875, *System Authorization Access Request (SAAR)*

***Abbreviations and Acronyms***

**ABMS**—Advanced Battle Management System

**ACAS**—Assured Compliance Assessment Solution

**ADSV**—DeviceOne Secureview

**AF**—Air Force

**AF EPL**—Air Force Evaluated Products Listing

**AFIN**—Air Force Information Network

**AFPD**—Air Force Publishing Directive

**AMAC**—AFIN Mission Assurance Center

**ANG**—Air National Guard

**AO**—Authorizing Official

**ARW**—Application Request Worksheet

**ATC**—Approval to Connect

**ATO**—Authorization To Operate

**BSLM**—Base Software License Manager

**C2C**—Comply-To-Connect

**C-ISP**—Commercial Internet Service Provider

**CAC**—Common Access Card

**CCRI**—Command Cyber Readiness Inspection

**CFP**—Communications Focal Point

**C-ISP**—Commercial Internet Service Provider

**CIPS**—Cyberspace Infrastructure Planning System

**CompTIA**—Computing Technology Industry Association

**CORA**—Cyber Operational Readiness Assessment

**CPCON**—Cyberspace Protection Condition

**CL**—Cybersecurity Liaison

**CR**—Cyber Readiness

**CSS**—Commander's Support Staff

**CSSP**—Cyber Security Service Provider

**CST**—Client Systems Technician

**CTO**—Cyber Tasking Orders

**CUI**—Controlled Unclassified Information

**DCWF**—DoD Cyberspace Workforce Framework

**DAF**—Department of the Air Force

**DISA**—Defense Information Systems Agency

**DISN**—Defense Information Systems Network

**DLP**—Data Loss Prevention

**DoD**—Department of Defense

**DODIN**—Department of Defense Information Network

**eMASS**—Enterprise Mission Assurance Service

**ERM**—Electronic Records Management

**ESD**—Enterprise Service Desk

**ESS**—Endpoint Security Solution

**FIPS**—Federal Information Processing Standard

**FSA**—Functional System Administrator

**IA**—Information Assurance

**IAO**—Information Assurance Officer

**ISO**—Information System Owner

**ISP**—Internet Service Provider

**ISSM**—Information System Security Manager

**ISSO**—Information System Security Officer

**JBSA**—Joint Base San Antonio

**MAB**—MAC Authentication Bypass

**MAC**—Media Access Control

**MDE**—Microsoft Defender Endpoint

**MECM**—Microsoft Endpoint Configuration Manager

**MI-FI**—Mobile Wi-Fi

**MTO**—Maintenance Tasking Order

**NDCI**—Negligent Discharge of Classified Information

**NIPRNet**—Non-Secure Internet Protocol Router Network

**NIST**—National Institute of Standards and Technology

**NSI**—No Security Impact

**NOTAM**—Notices to Airmen Message

**NTFS**—New Technology File System

**OPR**—Office of Primary Responsibility

**OTL**—Over Threshold Limit

**PII**—Personally Identifiable Information

**PKI**—Public Key Infrastructure

**PM**—Program Manager

**PMO**—Program Management Office

**POA&M**—Plan Of Actions & Milestones

**PWS**—Performance Work Statement

**RMF**—Risk Management Framework

**SAR**—Security Access Requirement

**SAAR**—System Authorization Access Request

**SaaS**—Software as a Service

**SAV**—Staff Assistance Visit

**SBRC**—Scan Battle Rhythm Calendar

**SCCM**—System Center Configuration Manager

**SDC**—Standard Desktop Configuration

**SIPRNet**—Secure Internet Protocol Router Network

**SNAP**—Systems/Network Approval Process

**SOW**—Statement of Work

**SSD**—Solid-State Drive

**STIG**—Security Technical Implementation Guide

**TASKORD**—Task Order

**TRL**—Targeted Removal Listing

**UMD**—Unit Manning Document

**USB**—Universal Serial Bus

**USLM**—Unit Software License Manager

**VAT**—Vulnerability Assessment Technician

**VPN**—Virtual Private Network

**WCO**—Wing Cybersecurity Office

**WVI**—Weighted Vulnerability Index

***Office Symbols***

**502 ABW/CC**—502 Air Base Wing and Joint Base San Antonio Commander

**502 CS/CC**—502d Communications Squadron Commander

**502 CS/SCXS**—502d Communications Squadron Cybersecurity Office

**688 CW/A6**—Enterprise Access Management Organization

## Attachment 2

## ACCEPTABLE RULES OF BEHAVIOR

**Figure A2.1. JBSA Acceptable Rules of Behavior on Official Letterhead**

DEPARTMENT OF THE AIR FORCE
502D AIR BASE WING
JOINT BASE SAN ANTONIO

DATE (DD Mmm YY)

MEMORANDUM FOR Member's Sq /ISSO

FROM: Member's Name (First MI, Last)

SUBJECT: Rules of Behavior and Acceptable Use Standards for Information Technology for JBSA Lackland and Randolph Air Force Networks

1. The following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology. By signing below, I indicate both my understanding of these standards, and my agreement to act in accordance with them as condition of my service with or access within the Air Force. Air Force Instruction 17-130, *Cybersecurity Program Management* applies.

2. I WILL adhere to and actively support all legal, regulatory, and command requirements.

a. I understand that Air Force Information Technology is to be used primarily for Official/Government Business, and that limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems, or reflect adversely on the Air Force or the DoD.

b. I will not sue my access to government information or resources for private gain.

c. I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains.

d. I will observe all software license agreements and Federal Copyright laws.

e. I will encrypt and sign any messages containing For Official Use Only, Personally Identifiable Information, or Controlled Unclassified Information.

f. I will promptly report all security incidents in accordance with Air Force policy.

3. I WILL use the system in a manner that protects information confidentiality, integrity, and/or availability.

a. I will not store, or process classified information on any system not approved for classified processing.

b. I will protect my Common Access Card/hardware token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.

*Mission ~ Wingman ~ Partners*

c. I will protect my passwords/Personal Identification Numbers from disclosure: I will not post or write these down in my workspace.

d. I will lock or log-off my computer or terminal any time I walk away.

e. I understand that my password/Personal Identification Numbers must adhere to current Air Force standards for length, key-space, and aging requirements.

f. I will not disclose any non-public Air Force or DoD information to unauthorized individuals.

g. I understand that everything done using my Common Access Card/hardware token/password/Personal Identification Number will be regarded as having been done by me.

h. I will employ anti-malware software and update it as required; I will immediately notify my CFP or WCO if I believe Air Force Information Technology assets entrusted to me have been compromised; I will take immediate measures to limit damage.

4. I WILL protect the physical integrity of computing resources entrusted to my custody or use.

a. I will protect Air Force Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.

b. I will protect Air Force Information Technology from tampering, theft, or loss; I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.

c. I will protect Air Force Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of information contained, and practice proper labeling procedures.

d. I will not allow anyone to enter DoD or Air Force facilities without proper authorization.

e. I will not install, relocate, modify, or remove any Air Force Information Technology without proper approval.

5. I WILL NOT attempt to exceed my authorized privileges.

a. I will not access, research, or change any account, file, record, or application not required to perform my job.

b. I will not modify the operating system configuration on Air Force Information Technology without proper approval.

c. I will not move equipment, add, or exchange system components without authorization by the appropriate approval of my local systems manager or local hardware custodial personnel.

d. I will not use, or connect to, non-official hardware, software, or networks for official business without proper approval and without the use of authorized mobile device network encryption.

6. I WILL NOT use systems in a way that brings discredit on Air Force users or the Air force; or degrade the Air Force missions.

*Mission ~ Wingman ~ Partners*

a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.

b. I will not receive or send inappropriate material using my official email or Internet accounts.

c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral, or philosophical agenda.

d. I will not add slogans, quotes, or other personalization to an official signature block.

e. I understand that pornography, sexually explicit or sexually oriented material, nudity, hate speech, or ridicule of others based on protected class (e.g., race, creed, religious, color, age, sex, disability, national origin), gambling, illegal weapons, militant, extremist, or terrorist activities will not be tolerated.

f. I will not connect or remove any form of removable media without proper approval.

7. I WILL NOT waste system and network resources.

a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook®, Twitter®, Instagram®, Snapchat®, etc.).

b. I will not make excessive use of my official computer for shopping, or to view full-motion videos from non-official sources (e.g., YouTube®, online multiplayer video games, etc.).

c. I will not auto-forward e-mail from my official account to a personal e-mail account.

8. This memo will be kept on file with member's ISSO until one year after member leaves the unit.

X

Member's Name
Member's Squadron

*Mission ~ Wingman ~ Partners*