BY ORDER OF THE COMMANDER
YOKOTA AIR BASE

YOKOTA AIR BASE INSTRUCTION
17-101

19 NOVEMBER 2019

Cyberspace

COMMUNICATION
SQUADRON CUSTOMER SERVICES

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: 374 CS/SCXP

Certified by: 374 MSG/CC
(Colonel Tanya J. Anderson)

Pages: 23

This instruction implements AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*. It provides guidance and procedures on service restoration, network management, developing work orders, managing information technology systems, cybersecurity services, and requests for public address. It applies to individuals at all levels at Yokota Air Base, except where noted otherwise. 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. Refer recommended changes and questions about this publication to the OPR listed above using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System, Records Disposition Schedule. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

Chapter 1

ROLES AND RESPONSIBILITIES

1.1. Installation Commander will:

1.1.1. Ensure compliance with this instruction.

1.1.2. Appoint a Base Communications and Information Systems Officer (CSO) in writing.

1.2. Base Communications and Information Systems Officer will:

1.2.1. Serve as the Host Accountable Property Officer (APO) IAW AFMAN 17-1203.

1.2.2. Appoint the following primary and alternate positions in writing:

1.2.2.1. Base Equipment Control Officer (BECO).

1.2.2.2. Base Software License Manager (BSLM).

1.2.2.3. Command, Control, Computers, and Communications (C4) Requirements Manager.

1.2.2.4. Installation Information System Security Manager.

1.2.3. Be approval authority for off-station public address requests.

1.2.4. Be approval authority for mailbox size limit increase requests (see **Attachment 2**).

1.3. Base Equipment Control Officer:

1.3.1. Also known as the Equipment Control Officers (ECO), the Base Equipment Control Officer (BECO) must be at least E-5 or civilian equivalent and those who are appointed to the BECO office are the subject matter expert on all things related to the overall management of the information technology (IT) assets managed on Yokota Air Base.

1.3.1.1. Information Technology Asset Management (ITAM). The BECO oversees procurement and inventory management of end user devices such as computers, printers, iPhones, etc. IAW AFMAN 17-1203.

1.3.1.2. Personal Wireless Communication Services (PWCS). The BECO oversees procurement and inventory management of all PWCS devices such as land mobile radios (LMRs) and will comply with all requirements IAW AFI 17-210, *Radio Management*. Unit ECOs or CC-directed personnel may contact the BECO office for assistance with PWCS procurement and inventory management.

1.3.2. Unit APO and property custodians (PC), also referred to as Equipment Custodians (EC), are responsible for maintaining accountability of all equipment they have assigned to their inventory, and for complying with BECO-directed inventory activities. The BECO will work with the PC to resolve account discrepancies. Accounts that are not current will be locked, and procurement of new equipment and account adjustments will not be authorized until discrepancies are resolved. When inventories are required, the BECO will typically contact the PC with the following procedure:

1.3.2.1. Initial e-mail will be sent to the PC 45-60 days before the account is due to be reconciled.

1.3.2.2. Follow-up e-mail sent to the PC 30 days before an account is due.

1.3.2.3. Final e-mail sent at 15 days before an account is due, with the owning unit commander or equivalent, and the CSO copied on e-mail correspondence.

1.4. Base Software License Manager:

1.4.1. Ensure annual inventories are conducted for all non-enterprise software licenses for all organizations under BSLM purview.

1.4.2. Collect an annual baseline inventory for all non-enterprise software licenses.

1.4.3. Provide annual inventories to higher headquarters as required or as requested.

1.5. Command, Control, Computers and Communications (C4) Requirements Manager:

1.5.1. Provide vetting, technical solutions, and cost for customer requested C4 requirements.

1.5.2. Appoint a project manager for long-term C4 projects when necessary.

1.5.3. Manage installation C4 strategic priorities and annual requirements documentation submission in coordination with the Air Force Installation Mission Support Command, PACAF A3/6, and the 38th Cyberspace Engineering and Installation Group.

1.5.4. Manage installation Cybersecurity Representative (CR) program, including training, policy development, and information dissemination.

1.6. Installation Information System Security Manager:

1.6.1. Primary cybersecurity technical advisor to the CSO for all network activities.

1.6.2. Ensure CRs are trained on cybersecurity functions, including submitting change requests and communication work orders.

1.6.3. Develop an incident response plan in the event of a cybersecurity incident occurrence.

1.6.4. Track and maintain data loss prevention (external hard drive) waivers and USB violations.

1.6.5. Implement and enforce all AF cybersecurity policies, procedures and counter measures.

1.6.6. Process and coordinate cybersecurity waivers for network policy exemptions. An exemption to network policy must first be submitted as a work order in Cyberspace Infrastructure Planning System (CIPS) prior to the waiver process.

1.6.7. Manage the Wing Computer Security, communication security, and TEMPEST programs.

1.6.8. Ensure security control compliance throughout the Yokota Air Base network to authorized endpoint devices. New IT devices cannot access the network until the risk management framework process for assessment and accreditation has been completed and authorized the device.

1.6.9. Conduct annual COMPUSEC self-assessments.

1.7. Unit Commander’s or Equivalent Responsibilities:

1.7.1. Ensure their organization complies with this instruction.

1.7.2. Serve as the Unit Accountable Property Officer (APO) and Property Custodian as outlined in AFMAN 17-1203.

1.7.3. Appoint the following positions in writing:

1.7.3.1. A Primary and Alternate CR to manage the unit's communication requirements. Appointment letters must be submitted to the Wing Cybersecurity Office (WCO) (see **attachment 3**).

1.7.3.2. A primary and at least one alternate Property Custodian(s) for each accountable area designated, as outlined in DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*.

1.7.3.3. Unit Software License Manager (USLM) if required to assist in carrying out responsibilities as the Unit APO.

1.7.4. Validate funding for Work Order requests submitted through CIPS for CS planning and implementation.

1.8. Unit Cybersecurity Representative:

1.8.1. Formerly knowns as Cybersecurity Liaisons (CSLs), Information Assurance Officers, and Telephone Control Officers. Units will appoint at least one primary and one alternate CR to serve as the primary focal point for all C4 issues and work orders for each unit. CRs are responsible for all administrative cybersecurity tasks as directed by the Wing Cybersecurity Office (WCO), submitting C4 Work Orders through CIPS, and representing their unit's C4 concerns to the host base communications squadron, IAW AFI 17-130, *Cybersecurity Program Management*. Duties may be separated among multiple CRs for larger squadrons. Cybersecurity Representatives (CRs) are responsible for the following:

1.8.2. Training for CRs is required upon appointment and recurring annually by the WCO.

1.8.3. Unit CRs will be inspected by the Management Internal Control Toolset Self-Assessment Checklist for AFMAN 17-1301, *Computer Security*.

1.8.4. The CR will coordinate with CFP for the following:

1.8.4.1. Submission of trouble tickets not resolved with the Virtual Enterprise Service Desk (vESD) (see **paragraph 2.1.3**.).

1.8.4.2. User account request and provisioning.

1.8.4.3. In the event of a security incident.

1.9. Property Custodian's Responsibilities:

1.9.1. Also known as Equipment Custodian, PCs will complete all training outlined by the Asset Management office, including refresher training.

1.9.2. Property custodians will complete an inventory when one of the following occurs:

1.9.2.1. The primary PC undergoes a permanent change of station or permanent change of assignment from their unit.

1.9.2.2. Perform an inventory review annually.

1.9.2.3. As directed by the BECO.

1.9.3. Property custodians will submit a new appointment letter any time there are personnel 4 Notify the BECO office of any changes or missing items so those assets can be properly accounted for through a Report of Survey (ROS) or an Accountable Property Inventory Adjustment Worksheet. Administrative action per owning unit commander may be taken against PCs who are unable to locate missing equipment following ROS report and findings.

1.10. Unit Software License Manager:

1.10.1. Manage all software licenses owned by the organization in support of the base software license management program IAW AFMAN 17-1203.

1.10.2. Ensure applicable training is conducted for users in support of unique software purchased or developed.

1.10.3. Identify enterprise software license requirements and any management training requirements not covered in existing courses to the BSLM for annual consolidation.

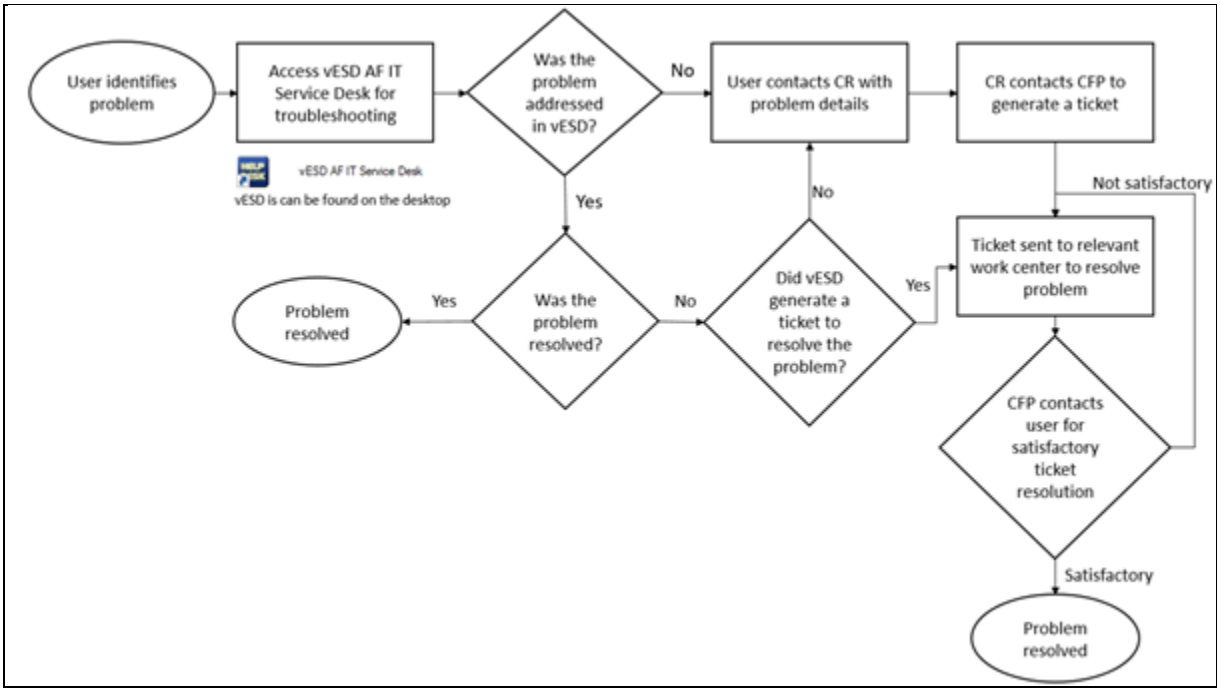
Chapter 2

SERVICE RESTORATION AND NETWORK MAINTENANCE

2.1. Incident Management.

2.1.1. IT systems, such as computers, phones, and software will not always work as intended for end users. **Figure 2.1**. below depicts the typical troubleshooting and reporting process an end user will follow when they have a service incident with their IT equipment or service:

Figure 2.1. Troubleshooting Process.



2.1.2. Virtual Enterprise Service Desk (vESD) is an application on all AFNET computers that can resolve common technical issues that a user can experience, including the following:

2.1.2.1. E-mail.

2.1.2.2. External and internal network connectivity, including the world wide web.

2.1.2.3. Hardware.

2.1.2.4. Software.

2.1.2.5. Desk and mobile phones.

2.1.2.6. Cyber Threats.

2.1.3. In the event that vESD cannot resolve a user's technical issue and is unable to generate a trouble ticket, the CR may contact the Communications Focal Point (CFP) at 225-2666, option 2.

2.1.4. IT service incidents can have significant impact on mission accomplishment. It is important that incidents are appropriately categorized in order to assign proper priority to generate response and resolution activities. It is important the CRs provide as much information as possible to the CFP when an incident occurs. This information includes administrative data such as network, location, users impacted, etc., as well as mission(s) impacted. **Table 2.1**. below provides service request priorities, examples, and response times:

Table 2.1. Service Request 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; distinguished visitor support	Immediate/4 Hours/24x7
High	Base isolation; base-wide core service outage; any outage affecting an O-6, E-9, GS-15, and/or higher	30 Mins/8 Hours/24x7
Medium	Issues causing work-stoppage affecting multiple users; degraded base-wide network capabilities	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)

2.2. Network Maintenance Window.

2.2.1. In order to keep networks and IT equipment working optimally, the CS must complete maintenance requiring network down time and service unavailability. Network maintenance windows for NIPR devices will occur weekly on Tuesdays and Thursdays, starting from 2200L until 0200L. During these periods, users may experience a degradation or outage of network services to include but not limited to:

2.2.1.1. Share drives.

2.2.1.2. Printing services.

2.2.1.3. World wide web availability.

2.2.1.4. Network access.

2.2.1.5. E-mail.

2.2.1.6. Virtual Private Network availability for off-station users.

2.2.2. A SIPR uptime will be enforced to mitigate network vulnerabilities and to keep IT equipment working optimally. SIPR network device owners will have their SIPR devices online from 0900L to 1500L on Tuesday and Wednesday every week.

2.2.2.1. Accountability and patching of all SIPR network devices, including PMO devices, will be conducted in this window. If a device is not online for two weeks of maintenance windows, the device will be locked.

2.2.2.1.1. The 1st Violation. To unlock the device, the device owner will be required to contact the CFP to submit a trouble ticket.

2.2.2.1.2. The 2nd Violation. Further violations will require a plan-of-action memorandum signed by the non-compliant unit's Commander and emailed to CS/CC and the CFP email org box.

2.2.2.1.3. The 3rd Violation. If the same device is locked again for being delinquent, it will remain locked until a plan-of-action is made between the non-compliant unit Commander and the CS/CC to meet the SIPR uptime requirement. This will be accomplished by replacing the delinquent device with an Enhanced-Virtual Desktop Infrastructure zero client or resolving the fault.

2.2.2.2. Enhanced-Virtual Desktop Infrastructure zero clients are exempt from the uptime. On Yokota Air Base, zero clients are small boxes with "EVGA" or "WYSE" displayed on the device. Contact the CFP to switch to zero clients to be exempt from this policy.

2.2.3. Exceptions. Should any user have a mission requirement that may preclude 374 CS from using the weekly maintenance window, the CFP should be contacted immediately in order to post-pone the maintenance window or coordinate alternate means of providing communications capabilities. The CFP can also be contacted after a maintenance window concludes if service unavailability persists.

2.3. Authorized Service Interruption.

2.3.1. An authorized service interruption (ASI) is a scheduled period of downtime to network, equipment, systems, or services to perform maintenance, upgrades, replacements, etc. ASIs are scheduled at a time that will have minimum impact on operations and notifications are sent immediately from the CFP when an ASI is scheduled.

2.3.2. Organizations must contact CFP through SIPR to initiate the ASI scheduling. The requesting organization must submit scheduling paperwork a minimum of 21 days prior to the intended ASI date for proper coordination and to prevent any delays.

2.3.3. Emergency ASIs are for events that require an immediate service interruption to correct a hazardous or degraded condition that cannot otherwise be scheduled as a routine service interruption. Emergency ASIs will be resolved as soon as possible to resume service activities.

Chapter 3

C4 REQUIREMENTS

3.1. Work Order Request Process.

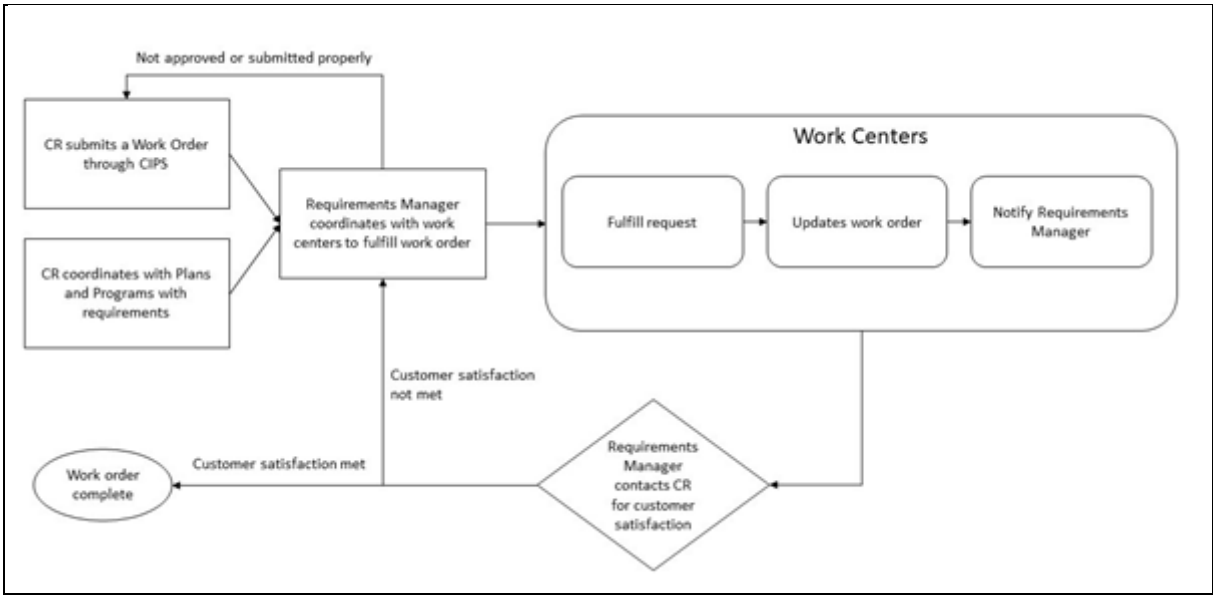
3.1.1. A C4 work order submitted into CIPS is used to process requests for new IT services and changes to existing IT services. Before a request can be accomplished it must be submitted into CIPS by a unit CR, and then approved through processes established by the C4 Requirements Manager. CRs must fill out the CIPS work order completely per training provided, or the work order will be returned. For guidance, contact Plans and Programs at 225-3850.

3.2. Work Order Processes.

3.2.1. After approval, a Work Order will be assigned a process, a priority, and a work order number. The three processes are standard, non-standard, and emergency work orders.

3.2.2. Standard Change Process. Standard Changes are preapproved, repetitive, low-risk, well-tested changes (e.g., new accounts, telephone changes/additions, email, small hardware, and standard software/system access requests).

Figure 3.1. Standard Change Process.



3.2.3. Non-Standard Change Process. A non-standard change can involve evaluation, planning, preparation, expense, service disruptions, and impact to other services or risks to security. A non-standard change, therefore, will take more time and may require additional funding by the customer.

Figure 3.2. Non-Standard Change Process.

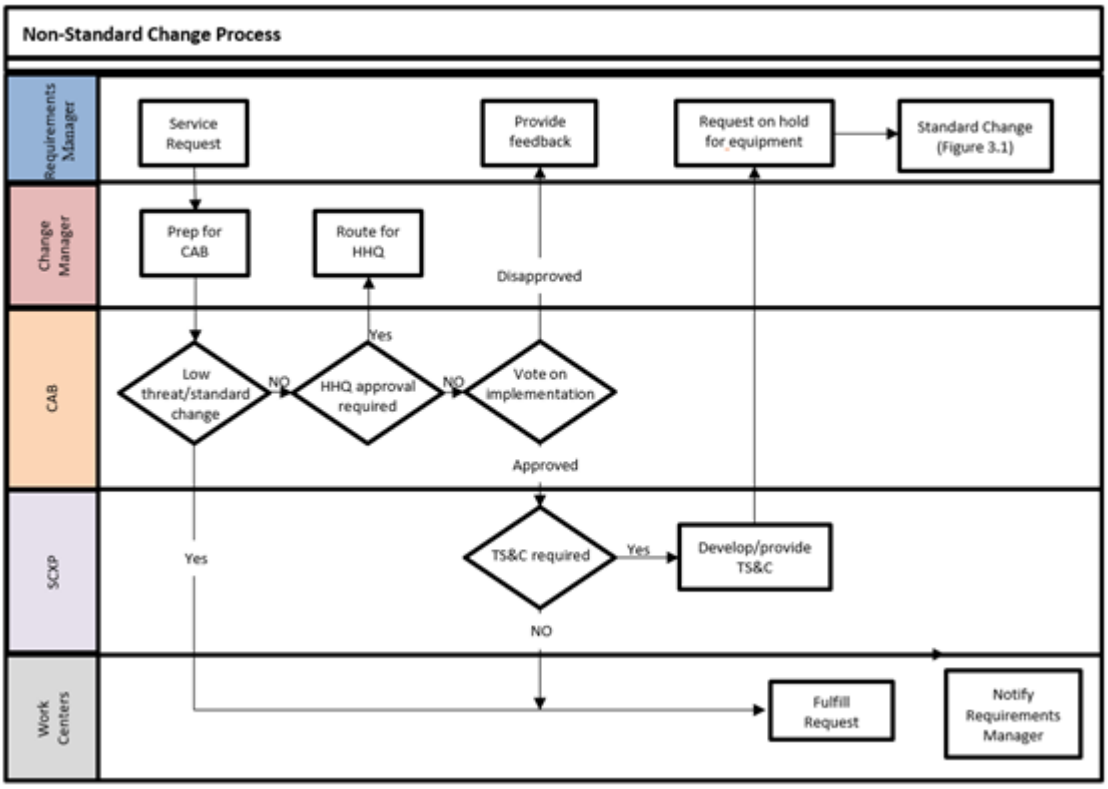


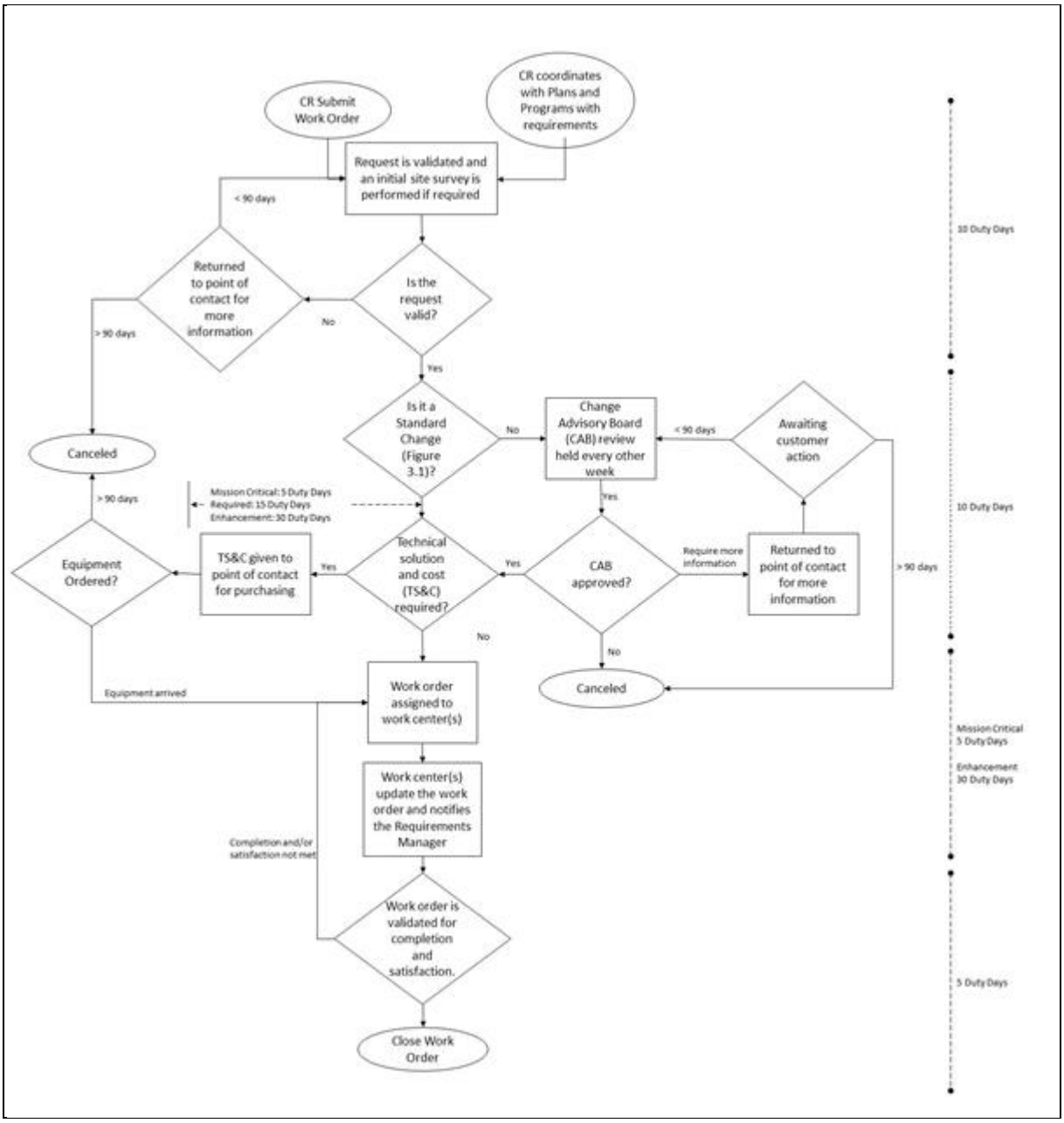
Table 3.1. Process Priority Timeline.

Priorities	**Standard Change Approximate Completion Timeline**	**Non-standard Change Approximate Completion Timeline**
Mission Critical	5 Days	10 Days
Required	15 Days	30 Days
Enhancement	30 Days	60 Days

3.2.4. Emergency Change Process. An Emergency Change is a change requiring immediate implementation to correct a major incident, security patch, or problem. Emergency changes require the approval of the 374 CS/CC to be implemented.

3.2.5. Upon completion of a change, an Air Force Technical Order Form 747, *Cyberspace Infrastructure System Acceptance*, is routed for project acceptance and certification.

Figure 3.3. Service Request Process.



Chapter 4

INVENTORY MANAGEMENT

4.1. Unit Procured Tech Refresh.

4.1.1. During inventory activities, Unit APOs or PCs are responsible for identifying assets that have expired warranties or are not currently meeting mission requirements. **Table 4.1**. below shows the recommended refresh rate for IT end items.

Table 4.1. Device Refresh Rate.

Device Type	Recommended
Desktop	5 years
Laptop	4 years
Tablet	4 years
Cell Phone	2 years
Printer: Standalone	5 years
Printer: Multi-Functional Device	5 years

4.1.2. PCs must use the Air Force Way web site (AFWAY) at **https://www.afway.af.mil** to initiate a unit-procured tech refresh.

4.1.2.1. Through AFWAY, the PC will be able to search in the products section for assets that meet their needs using guidance provided from the BECO as necessary. The BECO is an approval authority on AFWAY orders, and will provide guidance on computer types and models to ensure compliance with Yokota's networks.

4.1.2.2. If the asset is unable to be found in the product search window, the PC must open a Request for Quote (RFQ) and submit for approval. The PC must wait a minimum of three days for a response to the RFQ.

4.1.2.2.1. All IT equipment not purchased through AFWAY must go through the NETCENTS-2 contract for solutions that adhere to the AF Enterprise Architecture. RFQ for IT equipment that do not adhere to the AF Enterprise Architecture will be denied.

4.1.2.2.2. If an RFQ is not returned in a timely fashion, the PC may request a waiver to not use the AFWAY process.

4.1.2.3. When preparing an order for shipping, the PC must provide the following information in AFWAY:

4.1.2.3.1. Address Name: 374 CS SCOSA.

4.1.2.3.2. Building: 653 – 105.

4.1.2.3.3. Address 1: Yokota AB.

4.1.2.3.4. Address 2: APO AP 96328-5081.

4.1.2.3.5. City: Fussa.

4.1.2.3.6. State: Tokyo.

4.1.2.3.7. Zip: 1970001.

4.1.2.3.8. Country: Japan.

4.1.2.3.9. Marked for address: Requesting PC/Unit information.

4.1.2.4. Once all information is completely filled out, the PC will finalize the purchase in AFWAY.

4.1.2.5. When purchased equipment is delivered to 374 CS, a member of the BECO office will notify the PC. PCs will have 10 working days from the notification to retrieve their equipment before escalating notification to unit CCs.

4.1.2.6. When purchased equipment is delivered to the PC, a member of the BECO office will ensure all equipment serial numbers (Serialized Item Management and Item Unique Identification) are transcribed onto the proper documents/receipts IAW AFMAN 17-1203. After proper receipt and acceptance of hardware, the PC will then sign for accountability before taking possession of equipment.

4.1.2.7. If necessary, the PC must open a work order through their CR to have computers imaged.

4.2. Personal Wireless Communication Services.

4.2.1. Requesting Land Mobile Radios (LMRs).

4.2.1.1. The Asset Management office will reserve LMRs on a first come or priority basis.

4.2.1.1.1. In the event of a natural disaster, real world operations, or a major mishap, LMRs may be recalled.

4.2.1.2. Property Custodians must work with the unit CRs to submit a work order as early as possible to reserve a LMR with the required configurations.

4.2.1.3. The 374 CS requires at least one week's notice in order to plan and program LMR support, unless a natural disaster or real world operation requires immediate support.

4.2.2. Requesting Cell phones.

4.2.2.1. To purchase a cell phone, a CR must fill out a work order request in CIPS.

4.2.2.2. If the phone is not for a CC, CD, CEM, CCF, DO, flight leadership position or standby device, justification must be provided within the work order request.

4.2.2.3. The Asset Management office will coordinate with local vendors to provide a cell phone that meets requirements identified in the work order. Flip phones are typically provided for standby phones, as e-mail capability cannot be configured for multi-user mobile phones.

4.2.2.4. After a work order has been submitted, PCs will be contacted by a member of the BECO office to coordinate delivery.

4.3. Software License Management.

4.3.1. Software acquisition and software license acquisition.

4.3.1.1. All purchase requests must be initiated through a work order in CIPS, and approved by the BSLM.

4.3.1.2. Requested software must be on the AF Enterprise Product List (EPL) to be used on AF Networks. Programs not on the AF EPL are not authorized for purchase unless they are on an approved list IAW AFMAN 17-1203, paragraph 3.2.1. In this event, additional paperwork must be completed, but the end user will be assisted by the BECO in that process.

4.3.1.3. Software must be purchased from authorized existing DoD/AF Enterprise License Agreements: **http://www.esi.mil**.

4.3.2. Organizations will inventory all licensed software annually and submit to BSLM.

4.3.3. Organizations will dispose of all software IAW with AFMAN 17-1203 and submit documentation to BSLM.

Chapter 5

CYBERSECURITY SERVICES

5.1. Incidents/Violations.

5.1.1. Negligent Disclosure of Classified Information Reporting.

5.1.1.1. Classified Messages on NIPR. Users will follow the network reporting aid located on their Desktop. Users will contact their Security manager prior to contacting the CFP to confirm the classification of the message.

5.1.1.2. Classified Files on NIPR. Upon discovery of a file on NIPR that is classified, member will contact their Unit Security Manager and will notify the CFP.

5.1.2. To report a phishing email, the user will send the email as an attachment to the Yokota Wing Cybersecurity Office (**374aw.ia@us.af.mil**), or through their Security Manager.

5.1.3. If a user suspects a virus has infected any AF owned device, the networking reporting aid and immediately contact the CFP for action. The CFP will initiate the incident response actions. The Network Reporting Aid is located on all user desktops as a .pdf file.

5.1.4. Universal Serial Bus (USB) Violations.

5.1.4.1. USB Violations are frequently reported to the Wing Cybersecurity Office. A USB violation is defined as an unauthorized device willfully or negligently plugged into the Computer system through the USB port. Unauthorized devices are electronic items that have not been cleared through the WCO such as but not limited to external hard drives, cell phones, flash drives, etc.

5.1.4.1.1. The 1st Violation. Users will be immediately locked out from their user account and will only be reinstated access when the Cyber awareness challenge on Advanced Distributed Learning Service (ADLS) has been re-accomplished with the unit Cybersecurity representative, and their Unit Commander has signed the memorandum for record requesting account reinstatement for the user has been sent to the WCO.

5.1.4.1.2. The 2nd Violation. Users will be immediately locked out from their account and will only be reinstated access when the Cyber awareness challenge on ADLS has been re-accomplished with the unit Cybersecurity representative, and their Group Commander has signed the memorandum for record requesting account reinstatement for the user has been sent to the WCO.

5.1.4.1.3. The 3rd Violation. When the Cyber awareness challenge has been re-accomplished on ADLS with the unit Cybersecurity representative, and the 374 AW Commander has signed the memorandum for record requesting account reinstatement for the user has been sent to the WCO.

5.1.5. TEMPEST Violations/Incidents.

5.1.5.1. TEMPEST violations/incidents are situations/events that violate the integrity of the TEMPEST package. These are reportable security incidents. Violations/incidents include:

5.1.5.1.1. Wireless devices discovered in Classified Processing Areas.

5.1.5.1.2. Information Systems (IS) have been moved and violate approved TEMPEST distances.

5.1.5.1.2.1. **Exception:** Unit has an approved waiver from the Certified Technical TEMPEST Authority.

5.1.5.1.3. Classified Processing Areas that operate without an approved TEMPEST package.

5.1.6. Cybersecurity Incidents/Violations are defined as any action or actions that threaten the security of the network and/or its users. Any violations will be reported to the WCO and will be reported to the 374 CS/CC for risk determination.

5.1.7. User Agreement Violations/Incidents.

5.1.7.1. Information systems are a set of information resources. These devices include ISs such as desktop PCs, laptops, notebooks, smartphones, and mobile devices. All IS users will complete DOD IA training prior to granting access to an IS according to DOD 8570.01-M IA Workforce Improvement Program. Users will accomplish IA training annually using the Advanced Distributed Learning System computer based training which reports compliance.

5.1.7.2. All authorized IS users will sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision*, prior to initial IS access.

5.1.7.3. User's conduct that is inconsistent with the User Agreement may result in immediate suspension of access to unclassified and classified systems. Any violations will be reported to the WCO and will be reported to the 374 CS/CC for risk determination.

5.2. Data Loss Prevention Waivers (External Hard Drive).

5.2.1. Data Loss Prevention (DLP) Waivers also known as External Hard Drive Waivers. Unit CRs are responsible for tracking all hard drive exemptions within their Unit. All waivers must be processed by the CR prior to being sent to the WCO. The most up to date waiver template will be uploaded to the WCO SharePoint located at **https://yokota.eis.pacaf.af.mil/374AW/374MSG/374CS/374CSSCX/374CSSCXS/SitePages/COMPUSEC.aspx**.

5.2.2. All DLP waivers will include an Accountable Property System of Record inventory to ensure that the Hard drives are being tracked in an approved Air Force System.

Chapter 6

PUBLIC ADDRESS REQUEST

6.1. Radio Frequency Transmission (RF Trans) Work Center.

6.1.1. RF Trans will provide public address (PA) equipment, setup and support to official functions in which a group commander, equivalent or above is the presiding official.

6.1.2. RF Trans may provide portable sign-out equipment on a first-come, first-served basis for events below the threshold of support identified above.

6.1.2.1. Requests for PA support must be submitted at least four duty days prior to the event. The requesting unit will complete and submit a PA request located at the following link: **https://yokota.eis.pacaf.af.mil/374AW/374MSG/374CS/374CSSCO/374CSSCOTT/SitePages/Home.aspx**. Telephone contact can be made at 225-4461 for additional support.

6.1.2.2. RF Trans personnel will provide portable PA training at the time of equipment issue to ensure the POC can safely operate the equipment. Training includes power-on and power-off procedures, system setup and tear-down procedures, system adjustments and basic troubleshooting procedures.

6.1.2.3. Requesting units will sign for all equipment items on an AF Form 1297, Temporary Issue Receipt, at the time the equipment is borrowed. All equipment must be returned in the same condition it was issued. Cables should be tied or taped to prevent tangling and damage. The requesting unit POC is responsible to identify broken parts, problems, damage, or discrepancies when the equipment is returned.

6.1.2.4. PA equipment provided by the 374 CS can overheat if music is played continuously or if used for an extended amount of time in direct sunlight.

6.1.2.5. All equipment must be picked up at Building 653 NLT 1600 hours on the duty day prior to the even and returned NLT 1200 hours on the next duty day following the event unless mission requirements dictate otherwise.

6.1.3. Organizations with organic PA systems (i.e., Enlisted Club, Officer's Club, Taiyo Community Center, Base Theater, etc.) are responsible for setup and maintenance of their PA systems. RF Trans may assist with these systems as a courtesy, mission permitting.

6.1.4. Obtaining permanently installed PA equipment. Project must be initiated by a CR through a work order request in CIPS and should be accompanied by documentation of 374 CES work order approval.

OTIS C. JONES, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-360, *Publications and Forms Management*, 15 February 2018

AFI 17-130, *Cybersecurity Program Management*, 31 August 2015

AFI 17-210, *Radio Management*, 26 May 2016

AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*, 18 May 2018

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February, 2017

DODI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 31 August 2018

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

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

AFTO Form 747, *Cyberspace Infrastructure System Acceptance*

Abbreviations and Acronyms

ADLS—Advanced Distributed Learning Service

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFNET—Air Force Network

AFWAY—Air Force Way

APO—Accountable Property Officer

ASI—Authorized Service Interruptions

BECO—Base Equipment Control Officer

BSLM—Base Software License Manager

C4—Command, Control, Computers, and Communications

CFP—Communication Focal Point

CIPS—Cyberspace Infrastructure Planning System

CR—Cyberspace Representative

CS—Communications Squadron

CSO—Communications and Information Systems Officer

CSL—Cybersecurity Liaison

DLP—Data Loss Prevention

DOD—Department of Defense

EPL—Enterprise Product List

IAW—In Accordance with

IT—Information Technology

ITAM—IT Asset Management

LMR—Land Mobile Radio

NIPR—Non-secure Internet Protocol Router

OPR—Office of Primary Responsibility

PA—Public Address

PACAF—Pacific Air Forces

PC—Property Custodian

PWCS—Personal Wireless Communication Services

RF Trans—Radio Frequency Transmission

RFQ—Request for Quote

ROS—Report of Survey

SIPR—Secure Internet Protocol Router

SLA—Service Level Agreement

TS&C—Technical Solution and Costing

USB—Universal Serial Bus

USLM—Unit Software License Manager

vESD—Virtual Enterprise Service Desk

WCO—Wing Cybersecurity Office

Attachment 2

MAIL STORAGE LIMIT INCREASE MEMORANDUM TEMPLATE

Figure A2.1. Mail Storage Limit Increase Memorandum Template.

MEMORANDUM FOR 374 CS/CC
FROM: Requesting Organization
SUBJECT: Yokota Electronic Mail Storage Limit Increase

1. This waiver is to request an increase in electronic mail storage for NAME/EDI NUMBER IAW 690th Network Support Group Special Instruction-1, Appendix M, paragraph M4. Previous user was set to [select only one] category 1 (1 GB) / category 2 (500 MB) / category 3 (100 MB) and hereby requests storage increase to [select only one] category 1 (1 GB) / category 2 (500 MB) / other [specify size limit, will require 24 AF approval].

2. Justification for increased mailbox size [NOTE: lack of training on use of offline mail storage such as PSTs may not be used as justification. Contact 374 CS for training before submitting waiver].

3. I understand that this request exceeds the normal limits set forth in the 690th Network Support Group Special Instruction-1, Appendix M and must be processed through Yokota network change management, and signed by the 374th Communications Squadron Commander for mailbox sizes up to 1GB, and coordinated by the supporting Enterprise Service Unit Commander for mailboxes larger than 1GB.

Commander's Signature Block
Requesting Organization

1st Ind, 374 CS/CC

MEMORANDUM FOR 561 NOS Det1/CC

Concur/Nonconcur.

SCOTT A. METZLER, Lt Col, USAF
Commander

Attachment 3

CYBERSECURITY REPRESENTATIVE APPOINTMENT TEMPLATE

Figure A3.1. Cybersecurity Representative Appointment Template.

MEMORANDUM FOR YOKOTA CYBERSECURITY OFFICE
FROM: Organization/CSS
SUBJECT: Organizational Cybersecurity Duties

1. In accordance with AFMAN 17-1301, *Computer Security* (10 Feb 2017) and AFI 17-130, *Cybersecurity Management* (19 Mar 18), the following individuals are US citizens and are appointed as the organizational Cybersecurity Representive for Organizations Name located in bldg(s) _____.

Rank Last, First M.I.	DSN Phone Number	Office Symbol	DEROS

2. Appointed individuals have read and thoroughly understand the duties and responsibilities of the organizational Cybersecurity Representative as outlined in AFMAN 17-1301 and AFI 17-130 Para 2.17.

3. The primary Cybersecurity Representative in your unit will not be relieved of their responsibilities until the incoming organizational Cybersecurity Representative has been trained and a new appointment letter has been accomplished.

4. This letter supersedes all previous letters, same subject.

_____
_____
Signature of Primary Cybersecurity Representative Signature of Alternate Representative

(If each CR works in the CSS you do not need the commanders approval. This form can be signed by the NCOIC.) Delete this prior to completion.

FIRST M. LAST, RANK, USAF
Commander
Organization Name