Enclosure 42

Chapter 8
Portable Electronic Device Exception to Policy Process

8-1. Purpose

a. ETPs are required to allow PEDs into USASOC facilities (see chapter 4).

b. Any usage outside of the ETP justification is not allowed.

c. The ETP justification section must:

(1) *Identify the device.* "Medically required" is adequate identification for medically prescribed devices.

(2) *Specify the functions required*. For medically prescribed devices identify communication capabilities (cellular, Bluetooth).

(3) Provide all reasons the device and the functions requested cannot be met with available resources.

d. Visitors should submit an ETP request memorandum to the USASOC HQ G-632 a minimum of 48 hours before visiting. Visitors will follow section 8-2 of this regulation to request ETP.

e. G-22 SSO coordination is required if entering and/or exiting a special restricted facility (TSWAs, SCIFs, SAPFs, STOs).

f. USASOC HQ G-6 ISSM approval is required for all Bluetooth devices other than personal wearable fitness devices meeting requirements of chapter 4.

g. To bring the device into USASOC facilities:

(1) The ETP must be approved, and the device must be accompanied by a copy of the approved ETP.

(2) Except for medical devices, the ETP must be registered in the promoted links on the USASOC HQ G-632, Operations Cybersecurity portal page.

8-2. Procedure for exception to policy application

An ETP memorandum template and the ETP process are in the promoted links on the G-632 Operations, Cybersecurity branch portal page. Contact USASOC HQ G-632, Operations, Cybersecurity if additional assistance is required. Under rare circumstances, organizations may request a combined ETP for equipment regularly used by a group of people (for example Public Affairs Office (PAO)). Combined ETPs will list all equipment and all users and will be reviewed annually or when personnel or equipment change, whichever occurs first. Combined ETPs will be sparingly issued at the discretion of the G-2 and the G-6.

8-3. Annual reviews

Every 12 months, users will submit their ETPs, for re-approval to the G-22, G-34 and G-6. All ETPs will be reviewed, including medical devices and combined ETPs.

Chapter 9
Security Incident Response Procedures

9-1. Purpose

a. Cybersecurity incidents conducted by malicious actors and foreign governments present numerous threats to the DoD Information Network.

b. Security and cybersecurity incidents created through inadvertent, negligent, or willful acts of personnel must be addressed to clarify the situation, correct actions, and protect information.

c. This chapter establishes USASOC procedure for cybersecurity incident:

(1) Prevention.

(2) Reporting.

(3) Management.

(4) Remediation and disciplinary actions.

d. USASOC networks and information require the following:

(1) Protection from insider threats, malware, and cyber-attacks.

(2) Security relying on proper reporting, investigating, and incident handling.

(3) All network users having a favorable background investigation, an appropriate security clearance or access approvals, and access only to systems and information matching or below their clearance

9-2. Prevention

a. The following are in place to prevent cybersecurity violations:

(1) Cybersecurity policies and regulations.

(2) USASOC IT User Agreement.
(3) Cybersecurity awareness information (such as computer screensavers, posted security reminders).
(4) Annual cybersecurity awareness training.
(5) Approved procedures for moving information from one classification level to another.
(6) Required use of two-person integrity to verify information moved is not classified higher than the destination network to prevent NDCIs or spillage.

b. The only USB devices authorized to connect to Government networks are:
(1) Government or personally owned, wired:
(a) Mice.
(b) Keyboards.
(c) Common access card or token readers.
(d) Network web cameras with no memory.
(2) Government owned and USASOC AHL listed, wired (The USASOC AHL may be found on USASOC HQ G-632 Operations, Cybersecurity portal page:
(a) DTA authorized and exempt external hard drives.
(b) External CD devices.
(c) External DVR devices.
(d) Approved headphones (see chapter 4).
(3) DTA authorized wireless presentation remotes with an ETP.

c. Monitors connecting to government IS must:
(1) Be government furnished and on the AHL.
(2) Be personally owned with no capacity to store data or read data cards or drives.
(3) Not be smart televisions.

d. Proper procedures for moving information across classification levels must be followed.
(1) *For photographs:*
(a) Any Government furnished digital camera, regardless of classification, requires an ETP (see chapter 9) before connecting to a networked computer.
(b) An exclusive use stand-alone computer can be used to download and burn pictures to a CD/DVD for transfer without an ETP. See USSOCOM M380-3, Cybersecurity for additional information.
(2) *NIPR Data Transfer:*
(a) Data may be burned to CD/DVD-ROM.
(b) Data may be e-mailed from SOF network-unclassified (SOFNET-U) to either SOF Network-Secret (SOFNET-S) or Special Operations Command Research, Analysis and Threat Evaluation System (SOCRATES) systems using DOD Intelligence Information System One-Way Transfer Service at https://dots.dodiis.mil.
(c) Unclassified data may be moved from SOFNET-S to SOFNET-U using Combined Enterprise Regional Information Exchange System, http://www.centrixs.centcom.smil.mil/CFTS.cfm. All files must be marked with the appropriate security classification before initiating the transfer.
(d) Large amounts of data may be moved using an authorized and exempt external hard drive.
(3) *Classified Data Transfer:*
(a) Must be conducted by a DTA.
(b) Burning data to CD/DVD-ROM on classified networks (SIPR, SOFNET-S) must follow the data transfer process.
(c) Large amounts of data will be moved using authorized and exempt SIPR external hard drives if the mission requires.
(4) *Data transfer to and from mission critical weapons systems and DoD networks:*
(a) May require an air-gap solution to include the transfer of data to and from flash media (thumb drives, memory sticks) and DoD networks.
(b) See USSOCOM Manual 380-3 for additional information.
(c) Requestor must maintain a log of all file transfers for auditing purposes.

9-3. Security infractions and violations

Cybersecurity infractions and violations may generate a security incident report to the USASOC HQ DCS, G-22/G-34 and may trigger a USSOCOM cybersecurity incident report. Violations include, but are not limited to, actions listed in table 9-1.

Table 9-1.
Examples of Cybersecurity Infractions and Violations.

Security Infractions:	**Examples:**
Accessing prohibited Internet content, including but not limited to:	• Violence • Commercial activities • Gambling • Gaming • Hate • Known hacking/malware sites • Online storage • Auctions (e.g. eBay, Government surplus) • Person to Person file sharing • Racism • Selling • Soliciting • Terrorism • Unofficial advertising • Pornography • Violation of statute or regulation • Unauthorized/unapproved chat/instant messaging • Other uses incompatible with public service
Abusing privileged user access for non-related tasks, to include:	• Disabling or removing security/protective software or mechanisms and associated logs • Using elevated privileges to conduct user level tasks • Knowingly enabling security settings to bypass security measures (such as enabling ports or locked accounts) • Browsing the internet with elevated credentials • Modifying systems involved in an incident response event
Processing unauthorized Software:	• Uploading • E-mailing • Downloading
Security Infractions:	• **Examples:**
Using or possessing unauthorized PEDs or other unauthorized electronic devices in USASOC facilities:	• Entering with or using unauthorized electronic equipment in USASOC facilities • Using Government issued mobile devices within USASOC facilities without approval or proper documents
Connecting unauthorized devices to Government IS to include, but not limited to:	• CPEDs, with active ETPs, unless specifically stated in the ETP and the device is added to the network exemption group • Personally owned devices except headphones meeting chapter 4 requirements • Personal wearable fitness devices • Any non-Government owned device, even with an active ETP.
For any CSfC device or Government cell phone:	• Evidence of tampering • Unauthorized access • Loss or Theft
Spilling information or NDCI including on digital senders and scanners	• Equipment configuration files (e.g., SOF Deployable Nodes, Tactical local area networks configuration files) • Any files not intended for public release
CDV	• connecting an authorized device to a network of different classification
Taking unauthorized photographs or recordings	
Violating information assurance rules and regulations	

9-4. Reporting

a. Users who suspect and/or observe an unusual incident will:

(1) Cease all activities.

(2) Not leave the device unattended/unsecured.

(3) Immediately notify:

(a) System administrator/network administrator.

(b) Local unit ISSO.

(c) ISSM.

(d) G-6/S-6.

(e) Chain of command.

(f) USASOC G-3X SAPCO, if in SAPF.

(4) Refer to USASOC HQ G-6 cybersecurity portal (https://usasoc.sof.socom.mil/sites/usasoc-hq-g6/od/Cyber/default.aspx), SOP for Spillage promoted link for additional information.

b. CSC and CSU, G-6/S-6 designated ISSO representative will report NDCIs to RCSIRT.

c. Reports must have a CR (Incident – Submit a trouble ticket) in Remedy; they will be routed as follows:

(1) Completed by the CSC/CSU, G-6/S-6 ISSM/ISSO/or Information Management Officer.

(2) Returned to USASOC Cybersecurity Network Defense (CND) team for review.

(3) Submitted by USASOC CND, in final form, to RCSIRT for closure via USSOCOM Cyber Security Incident Response Team.

d. Units will not submit final reports directly to USSOCOM Cyber Security Incident Response Team for closure.

(4) Refer to USASOC HQ G-6 cybersecurity portal, Security Incidents promoted link for additional information.

9-5. Management

a. Upon notification of any cybersecurity incident, CSC and CSUs G-6/S-6 designated ISSO will immediately initiate an inquiry.

b. For each inquiry the CSC and CSU ISSO will:

(1) Suspend all the user's accounts within four hours, blocking access to all government networks.

(2) Investigate the incident.

(3) Provide resolution within 24 hours.

(4) Coordinate investigation with the incident report provided by USSOCOM and/or USASOC G-6, Operations Cybersecurity personnel. Collaborate with appropriate POCs to provide a complete investigation.

(5) Coordinate with the chain of command to determine if a formal investigation is required after considering the type and circumstances of incident.

(6) Evaluate the incident and draft a memorandum for record (MFR) including details and recommended disciplinary actions for the signature of appropriate leadership. See Appendix D for requirements and example memorandum.

(7) Courtesy copy USASOC HQ G22 information security and personnel security (PERSEC) POCs.

c. If a formal investigation is warranted, commanders and supervisors will consult with USASOC Office of the Staff Judge Advocate (OSJA) and personnel offices regarding the potential discipline of DOD users, and available actions regarding non-DoD users.

d. Suspected regulation violators may have their individual workspaces within USASOC facilities searched. Unauthorized devices are subject to seizure.

e. Search and seizures will be accomplished via proper channels (G-22, G-34, OSJA). The Cybersecurity team will promptly contact G-22, G-34, and/or OSJA POCs by e-mail and follow up with a phone call. These organizations will provide primary and alternate POC information in writing for off-duty hours.

f. G-2/S-2 PERSEC will be sent a DA Form 5248-R if required.

g. G-2/S-2 PERSEC will receive and review the DA Form 5248-R. The review will include:

(1) The nature, extent, and seriousness of the circumstances.

(2) If reporting was voluntary.

(3) Truthfulness and completeness in responding to questions.

(4) If the employee sought help and followed professional guidance.

(5) If employee demonstrated positive behavior changes.

9-6. Account suspension

a. Account suspension will remain in effect until all remediation is completed, documentation and the incident report have been received by USASOC Component Network Control Center (CNCC)/CND.

b. Account suspension will include the following steps:

(1) Will be initiated within four hours of incident report notification from any of the following USSOCOM, USASOC, U.S. Army Cyber Command, Defense Information Systems Agency, user, or observer.

(2) Will apply to connections through tactical local area networks involved including accounts, workstations, and devices.

(3) Suspended items will be disabled, isolated, and blocked.

c. Authority over accounts and personnel are held by the AO (ISSM for SOCRATES) and are as follows:

(1) Authority to suspend and remove user accounts from USASOC IS.

(2) For any data spillage, authority over military, Government civilians and contractors.

d. If a contractor is responsible for a data spillage, the COR will:

(1) Notify the employee's company.

(2) Notify the contracting officer.

(3) Confirm to the servicing SMO when notification is complete.

9-7. Investigation

a. Each incident report will include the five W's:

(1) Who: All parties involved.

(2) What: Describe the incident in as much detail as possible.

(3) When: Date of incident.

(4) Where: Networks (NIPR/SIPR/SOCRATES/Joint Worldwide Intelligence Communication System).

(5) Why: Describe how the event happened.

b. Information collected should be adequate to support evaluation of:

(1) Negligence levels:

(a) Willful: Purposefully disregards DOD security or information safeguarding policies or requirements. For example, intentionally bypassing a known security control.

(b) Negligent: Acts unreasonably in causing the spillage or unauthorized disclosure. For example, a careless lack of attention to detail or reckless disregard for proper procedures.

(c) Inadvertent: Did not know and had no reasonable basis to know, the security violation or unauthorized disclosure was occurring. For example, the person reasonably relied on improper markings.

(2) Insider risk.

(3) Appropriate remediation and disciplinary actions.

c. When determining negligence level, consider patterns of routine security violations due to:

(1) Lack of attention.

(2) Carelessness.

(3) A disregard for cybersecurity.

d. For each security incident, negligence levels will be taken into consideration when evaluating disciplinary actions, and recovery steps:

(1) The significance of the incident.

(2) The impact of the incident.

9-8. Disciplinary actions

a. Disciplinary actions will be evaluated with consideration of nature, frequency, severity, and negligence levels of the infraction(s)/violation(s).

b. Disciplinary actions may include:

(1) Prosecution under the Uniform Code of Military Justice.

(2) Adverse administrative actions.

(3) Other actions authorized by the United States Code of Federal regulations.

c. Insider threat designation will be based on the nature and number of cybersecurity incidents. A designation of insider threat may result in USASOC HQ G-6 leadership requesting account suspension or clearance revocation through the appropriate G-2/S-2 section.

d. USASOC military and civilian employees may be subject to the following:

(1) A verbal or written warning or reprimand.

(2) An incident report filed in the authorized system of record.

(3) Suspension of access to classified information.

(4) Removal or termination of employment.

e. Contractors: will be subject to possible removal from the contract.

f. Visitors or vendors: will be prohibited from entering USASOC facilities.

9-9. Remediation and account reinstatement measures

a. Users creating a cybersecurity incident are required to meet the following conditions:

(1) The CSC and CSU ISSO will draft a MFR as outlined in Appendix D, and the signed MFR will be inserted in the user's personnel file and attached to the incident report.

(2) The user must request limited access through an alternate account and retake annual cybersecurity awareness training and provide a copy of the certificate to their ISSO to accompany the incident report.

(3) The user must refresh and sign USASOC IT User Agreement and provide their ISSO a copy to accompany the incident report.

b. Specific steps and escalation for additional offenses is summarized in Appendix D-3.

c. Account reinstatement for a cybersecurity incident must be granted by USASOC HQ G-6 CND. Any other privileged user reinstating a locked account is committing a cybersecurity violation and will be investigated for abusing privileged user access. Reinstatement of privileged accounts may have addition requirements.

Chapter 10
Responsible and Effective Network Usage

10-1. Purpose

a. Personnel will use the internet to conduct official business. Dependency on networks requires safe and responsible use of all IS. All users are responsible for protecting themselves, their information, and USASOC information online.

b. Before a USASOC account is authorized for use, personnel must:

(1) Successfully complete Cyber Awareness Challenge (https://cs.signal.army.mil/).

(2) Read, sign, and follow USASOC IT User Agreement.

10-2. Internet threats

a. Internet use introduces many types of ongoing and constantly evolving threats to IS. Examples include but are not limited to malware, social engineering, eavesdropping, viruses, intelligence gathering, password attacks, spyware, phishing, and network attacks.

b. Each USASOC computer network user represents the first line of defense for protecting USASOC information and Special Operations Forces Information Environment.

c. Cybersecurity adversaries:

(1) May be internal or external to the organization.

(2) Vary in sophistication, access to resources, motivation, and intent.

d. Careless or ill-considered user actions also present risks. Content shared with the public should limit the possibility of:

(1) The user being victimized.

(2) Placing others in harm's way.

10-3. Information safeguards

a. The PAO is the only authorized release authority for the command and will post reviewed, approved, and releasable USASOC information on systems and websites that are publicly available.

b. Internet usage for all other users will follow:

(1) USASOC Policy 10-18, Acceptable Use of Social Networking Sites

(2) AR 360-1, The Army Public Affairs Program

(3) AR 530-1

(4) USSOCOM D 530-1

(5) AR 25-13, Army Telecommunications and Unified Capabilities

(6) USSOCOM M 380-3

(7) All Army activities (ALARACT) 061/2019, Professionalization of Online Conduct or subsequent issuance.

c. Internet use will not reflect adversely on USASOC or DoD. Prohibited examples include, but are not limited to, engaging in the activities listed in chapter 9, table 9-1 Examples of Security Infractions and Violations. These activities may trigger a cybersecurity incident (see chapter 9). Refer to USASOC policy 10-18, AR 25-13, AR 360-1, and DoD 5500.07-R, Joint Ethics Regulation for additional guidance.

d. All internet use will comply with DoD 5500.07-R which permits limited personal use of Federal Government resources when authorized on a non-interference basis.

e. When using Government furnished equipment, individuals will employ sound OPSEC following the guidelines in AR 530-1 and USSOCOM D530-1.

f. Collaborative applications (MS Teams, Wickr) will be used to support operations. When using collaborative applications, users will follow sound OPSEC guidelines. To include but not limited to:

(1) Turn on background blurring if using video.

(2) Utilize wired, government furnished headsets (see chapter 4) to mitigate inadvertent eaves dropping.

(3) When practical, place devices three meters (nine feet) from fixed radio frequency transmitters (radios or base stations, wireless fire or security alarm systems, wireless access points, wireless desktop computers, and portable (not cellular) telephones).

(4) Terminate communication if these guidelines are not followed.

(5) Notify your security manager immediately of violations.

g. Users will report spam and phishing promptly to CND at: https://sof.hq.socom.mil/Pages/ReportSpam.aspx

For further assistance regarding CSfC and Cybersecurity related issues contact: USASOC DCS, G-63 Operations Director or the USASOC DCS, G-632, Cybersecurity Branch, in Outlook USASOC.CYBERSECURITY@socom.mil or USASOC DCS G-636, Mobility branch.

For further assistance regarding TEMPEST or the certified TEMPEST technical authority, TSO or TEMPEST related issues contact: USASOC DCS, G-2, Security Operations Division.

For further assistance regarding information security and PERSEC contact:
USASOC G-22 TECH SEC, USASOCG2PERSEC@socom.mil or the USASOC DCS, G-2, Security Operations Division.