United States Antarctic Program

Computer Requirements for Connecting to the USAP Network

The United States Antarctic Program (USAP) addresses US federal government security and operational requirements for computing systems by screening *all* computers (including scientific/research instrumentation systems, mission operation systems, workstations, personal computers (PCs), servers, laptops, and portable notebooks) prior to connecting to the USAP network.

The following system requirements and operating system specifications apply to all participants desiring to connect to the USAP network with a non-USAP issued computing device, including bring your own device (BYOD), mobile devices (if authorized), and science equipment. Screening requirements apply to all participants who request access to USAP systems.

The latest information regarding USAP computer requirements, service, and infrastructure can also be found at https://www.usap.gov/usapgov/technology/index.cfm?m=4. Please direct inquiries to the USAP Help Desk at (720) 568-2001 or helpdesk@usap.gov.

To minimize wait time for computer screening, please ensure that your system meets the requirements identified in this document prior to deployment. Failure to comply with these guidelines may result in excessive delays or a denial of access.

A computer system must continuously maintain compliance with these computer requirements. A system that falls out of compliance (e.g., falls behind with anti-virus definitions, patches, or vulnerability remediation) may be disconnected without notice if the NSF determines there is an unacceptable level of risk or threat to the USAP environment.

System Requirements

Operating System and Software Patches

Device operating systems (OS) must be running on a version that is currently in accordance with USAP computer requirements and be updated with the most current patch level of the OS, including the most current security patches. Applications running on the system must also be patched when patches are released by the software vendor.

Antivirus

All devices must have antivirus software running at the current version and must be configured for automatic updates. Computers must be free of viruses prior to connecting to the USAP network and must maintain the current DAT version as updates are available.

Connectivity

Participants must provide all necessary equipment to connect the computer system to the USAP network, including the Network Interface Card (NIC), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.

Prohibited Protocols

Applications and software that utilize clear text are prohibited (e.g., Telnet, FTP, and Cisco SmartInstall), as they present a high risk to the USAP network. These protocols must be replaced with secure versions, such as SSH and SFTP.

Prohibited Actions

Prohibited actions include any activity designed to create an anonymous identity, inspect network traffic, determine vulnerabilities, and circumvent security or any other action that is not explicitly allowed or allowed by a Research Support Plan (RSP), including the following:

- Changing a MAC address
- Man-in-the-middle
- Sniffing and network scanning
- Utilizing credentials other than those provided
- Performing any action to circumvent enterprise security

Client and Server Software

Client software used for email and web browsing, as well SSH and SFTP software, are permitted. Software that is not permitted for use on the USAP network includes, but is not limited to, the following:

- Peer-to-peer (P2P) software (e.g., BitTorrent, KaZaA, Gnutella, Freenet)
- Email server software that provides SMTP/POP port services; some examples include Exchange, Eudora, and send mail.
- Web server software that provides HTTP/HTTPS/FTP services; some examples include IIS, Apache, and Lightppd.
- Network management servers, such as DNS and SNMP.
- Network or port scanning software, such as Nessus.
- Penetration tools such as Metasploit, BackTrack, and Wireshark.
- Unauthorized wireless access points and other network devices (firewalls, routers, etc.)
- Anonymizers or anonymous proxy tools

Software requiring NSF approval for use on the USAP network for official business purposes (such as educational outreach) includes Skype and other network bandwidth intensive applications, including video and audio streaming software.

Computer Screening Process

Screening technicians gather the information in the following table during the computer screening process. System operators who connect to the USAP network without a screening rating of "Pass" are in violation of USAP information security policy and may be disconnected without notice. A "Fail" rating indicates that the system owner is responsible for remediating the system as soon as possible to remain connected to the USAP network.

Data Collected By Computer Screening	
Owner's full name	All MAC addresses
Agency	OS version and patch level
Computer make and model	Antivirus software version and DAT file date
Computer hostname	Technician's name

For any concerns or clarifications, contact USAP-InformationSecurity@usap.gov.