FY-2006

Task A-03: Networking and Security Engineering and Operations
NASA Task TM: Richard Kurak

Task Summary:
The Office of Chief Information Office (OCIO) is responsible for providing total communications capabilities (voice, video, and data) for NASA GRC, and for providing ongoing support to various computer and communications research programs at GRC and throughout the Agency. Within OCIO, the Networking and Security Branch is responsible for the entire life cycle of all GRC communications systems and for keeping GRC at the "bleeding edge" of advanced network technology. The intent of this task is to provide network security support to the Networking and Security Branch in accomplishing its multifaceted mission.

Currently, network security support personnel use a host of IT hardware and software to preserve the integrity of the network. Hardware includes: Sun Workstations/Servers, Intel Workstations/Servers, Cisco routers, switches, Ethernet hubs, and concentrators. Software includes: Sun Solaris, Linux, Windows, Berkeley Internet Name Domain (BIND), Sendmail, Apache Web Server, CiscoWorks, CiscoSecure, Network Intrusion Detection, Proxy-based Firewalls, Intrusion Detection, Hacker deception tools, Secure Shell (SSH), Kerberos, and Secure Sockets Layer. Those supporting this task currently maintain servers in the internal security services network as well as distributed across the enterprise for various security purposes.

Subtask A-03.01: Networking and Security Engineering and Operations

NASA TM: Richard Kurak

Fiscal Year of Work: 2006 Funding Organization: VIE

Description

Overall Objectives:
Team PACE will provide engineering, implementation, administration, analysis and other daily support in the area of Center wide area and local area networking as well as Center security systems deployment and support. Operations will focus on meeting the security and networking requirements of the Center while maintaining a highly available and reliable network infrastructure. Team PACE will maintain a secured, available, and reliable IT infrastructure as approved by the Government.

Specific Work Requirements:
The Team will perform the following duties during the execution of this task:

- Operate and maintain the GRC network security environment while ensuring that the firewall system is operational 24 hours per day, 7 days per week. This includes the system administration and operation of all machines and software within the firewall including the web proxy server as well as those used to monitor network traffic.
- Operate and manage the GRC network gateway. Manage all access to the ESN and implementation of hosts and systems on the GRC External Services Network (ESN).
    - Operate and maintain an ESN web hosting service for GRC users. Provide network ports and access to the ESN as requested and approved.
    - Operate and maintain the border routers, switches, and interfaces to the Agency and public networks. This includes routing protocol configuration for our redundant links.
- Operate and manage the GRC Remote Access Infrastructure
    - Administer the GRC VPN services (currently Juniper SSL VPN and InfoExpress VTCP)
    - Transition all VPN users to the SSL VPN.
    - Admininster the GRS SSH proxy service.
    - Admininster the ACE Servers/SecurID systems.
- Work with NASA to meet changing requirements. Propose, test, and implement enhancements for NASA design specifications and IT Security Policies, and recommend solutions and implement them upon approval of the government. (The element requires that the resources are available from the government for the labor and equipment required in these endeavors).
- Identify equipment/software/services necessary for NASA GRC, and with appropriate government approval, obtain quotes from vendors, procure, and deliver necessary products to NASA GRC.
- Implement and maintain a data and systems backup solution to provide rapid recovery of applicable Networking and Security infrastructure.
- Monitor critical logs for abnormal activity and threat.
- Automated daily summary reports will be generated where available and distributed to the appropriate contractor and government personnel. Reports to GRC will be provided when threats are noticed as well as the appropriate external parties. Provide data/logs or a secure interface to the information in response to requests from appropriate parties.
- Provide requested technical documentation for existing and future network security system designs.
- Keep abreast of latest security threats and respond to any threats to the GRC network 24 hours a day, 7 days per week and take the appropriate actions to notify the designated government employee of threats,

then take the necessary steps to prevent further damage or intrusion. Actions should be initiated within 6 hours of discovery.

- Conduct forensic investigations of suspected IT Security incidents under the authority of the Center`s IT Security Manager or GRC Incident Response Coordinator. This may include, but is not limited to, the following: monitoring the network, examining and mirroring hard drive files, examining email files, reviewing network and firewall logs, disconnecting users` computers from the network, documenting the IT Security investigation, and providing testimony if required. The government will document the objective investigative tasks required of the technical personnel. Excluded from this task are any IT Security incidents categorized by the government as within the genre of computer and systems mis-use.
- Provide system logs related to misuse cases after approval of the contractor team lead and in a timeframe as resources permit
- Limited netcontext system administration.
- Vulerability scanning and reports to meet the Agency Quarterly scanning requirements. This will consist of monthly scans of the Agency list and a quarterly report.

- As resources permit or as funded directly by the customer, work with GRC users and customers to provide risk mitigated solutions that meet their requirements and maintain the security of NASA GRC.
    - Citrix server application hosting and user management.
    - VMWare systems management and virtual host implementation.
- Helpdesk Security queue monitoring and disposition.
    - ODIN Remedy Queue support for users interacting with Network Security systems.
- Provide network security support in the form of the elements listed below to the Telescience support center (TSC) and as agreed upon between OCIO/TSC management and the contractor and within the resources allowed.
    - Assist in the configuration and maintanence of the TSC firewalls.
    - Configure and maintain VPN hardware/software (currently Infoexpress VPN software) and user database.
    - Assist in maintaining the TSC firewall equipment in building 322 (currently includes: 2 - Cisco 2924 switches, 3 - Sun Ultra`s). Software and hardware support contracts are the responsibility of the TSC or TSC`s contractor.
    - Troubleshoot, diagnose, and support connectivity through the firewall for TSC IP traffic.
    - Provide network security engineering support and advice. Advise of risks and suggest alternatives for traffic that poses a threat to either the TSC mission network or the GRC Campus.
    - Attend meetings that are relevant to the work elements listed above as needed. Adhere to TSC change control requirements, procedures, and processes.

Additional efforts as funded and requested:

- **SSEB Networking, Security, and Support**
    - Assist in network engineering, testing, and implementation of SSEB networking or isolation network.

- **Extend and support a temporary VIP network on the ESN (LCNS Conference)**

- Engineering, configuration, testing, and support of the VIP network for the LCNS
    - Includes configuration of External Services Network to include a VLAN for the VIP(LCNS) network, additional ports and switches configured
    - Coordination with the GNOC and OCIO mgmt.
    - Implementation of a Linux DHCP server on a virtual machine
    - Configuration of a samba (Windows file sharing) server for file storage on the Linux box
    - Administration and patching of the server
    - Testing of the wireless networking
- Troubleshooting and diagnosis of the above components
- Clean up or removal of hardware and configuration at completion
- Attendance at meetings and availability during the conference

- **VPN Embedded System Design and Deployment**
    - Build a solid-state, embedded Soekris system to support visitor or guest networking needs from GRC locations that can not utilize fiber to the ESN or Open Networks.

End Products:
A highly reliable and available network infrasturcture and security architecture/implementation that protects, detects, and responds to the IT security threats of the Center while exceeding the operational requirements.

Assumptions:
- All network hardware, firmware, and software is provided by NASA GRC.
- All Team PACE employee workstation equipment is provided by NASA GRC.
- Travel & Training is on an "as required" basis, and funded by NASA GRC.

Deliverables:
- Documents, plans, presentations, drawings, designs and comments as necessary/requested.
- Integration, testing, and implementation of upgrades/infrastructure.
- Operations, maintenance, and support of the security infrastructure and WAN interfaces.
- Customer and user support to resolve issues for those interacting with the networking and security infrastructure.

Additional efforts as funded and requested:
- A temporary extension for the LCNS Conference to service visitors on a VIP wireless and wired network

Subtask A-03.02: IT Security Program, Policy, Audit, and Support

NASA TM: Richard Kurak

Fiscal Year of Work: 2006 Funding Organization: VP

Description

Overall Objectives:
Team will provide engineering, implementation, administration, analysis and other daily support in the area of IT security as well as program office support as it relates to customer outreach and plans/programs. Team will maintain a secured IT infrastructure as approved by the Government.

Specific Work Requirements:
Team PACE will provide engineering, implementation, administration, analysis and other daily support in the area of IT security as well as program office support as it relates to customer outreach and plans/programs. Team will maintain a secured IT infrastructure as approved by the Government.

Track and assist GRC Organizations in the Security Planning process.

- Work with Organizational Computer Security Representatives (OCSRs) to improve the overall security knowledge and posture of NASA GRC through layered defense strategies applied to systems within the GRC Network Perimeter.
- Facilitate and/or conduct IT security risk assessments for GRC Organizations, as requested
- Develop and maintain Center OAIT Master IT Security Plans and associated subordinate plans
- Documentation and updates as necessary to cover the stated work requirements
- Configuration Management efforts as they relate to the Center IT Security Program:
    - Audit and analysis of Center Patchlink data.
    - Physical access audits of the applicable networking and security spaces.
    - Configuration templates for workstation and server configurations. (Currently the CIS templates)
    - Respond to data calls and review policies from the Agency, other government organizations, and civilian authorities.
    - Conduct security reviews
    - Perform security controls audits
    - Perform analysis of FISMA, NPR, NIST, or other applicable documents or standards
    - Support the implementation and administration of the IT Security program at NASA GRC

End Products:
A team that provides the foundation for success in the plans, programs, and customer outreach activities of the IT Security Program Office.

Assumptions:

- All network hardware, firmware, and software to complete the necessary tasking is provided by NASA GRC.
- All Team employee workstation equipment is provided by NASA GRC.
- Travel & Training is on an "as required" basis, and funded applied separately by NASA GRC.