

TASK STATEMENT OF REQUIREMENTS (SOR)

Task Number: ARC004-10-00

Date: 20 June 2016

Task Title: Internal Operations

Requester: [REDACTED]

Period of Performance: August 1, 2016 through July 31, 2017

I Description of Work

The NAS Internal Operations Task provides infrastructure to the NAS Division projects and collocated staff in the NAS Network Domain. This grouping of work was created to provide consistent support across a broad spectrum of funding sources. This Task will support the Division and associated projects in these areas:

Subtask A: Program Management

Subtask B: Technical Marketing

Subtask C: IT Security for NAS Domain

Subtask D: Engineering Servers and Services

Subtask E: NAS Internal LAN

Subtask F: Facilities (Building, Physical Security, Property Management)

The NAS Internal Operations Task provides the common IT infrastructure for the NAS Building (N258) and NAS Domain residents [REDACTED]

[REDACTED] Various facility and IT services are provided depending upon the requirements of the Division.

Subtask A: Program Management

Government Point of Contact: [REDACTED]

This subtask area provides program management for all open tasks under this contract. Effective program management on the contract requires innovative approaches to optimise costs and maximize the Division's ability to pursue novel approaches for delivery of complete advanced modelling and simulation solutions to the Agency and mission directorates. In support of the Program Management requirements the contractor shall:

- Provide an interface between the contractor's management, the contractor's Task Leads, and the Government (Task Requestors, the COR, the CO, and the NAS Division.)
- Coordinate dissemination of technical information among various sub-tasks and maximize synergies among various technical areas under this Task Order.
- Employ state of the art methodologies and approaches in conduct of research, development and operation of NAS supercomputing assets and the delivery of services to its customers.

- Engage in developing a long-term vision to optimise costs and enhance the Division's ability to pursue its novel mission of support at competitive overall costs.
- Seek and employ highly qualified staff with significant accomplishments and with skill levels that will substantially impact progress in new areas of Division's activities.
- Strengthen current technical approaches by institutionalising modern software engineering practices and employing strong System Engineering principles.
- Monitor and trouble-shoot performance, delivery and documentation of milestones and deliverables in each task. Utilize automated management tools to assist with the processing of Task Assignments, tracking their performance, and documentation of work products.
- Ensure that the work products are meeting customers' expectations, design requirements and schedules. Perform all tasks at or below the indicated or approved budgets.
- Support the government in the procurement of ODC's in support of engineering and research requirements.
- Manage subcontracts supporting this contract in a seamless fashion focused on improving small business and technical goals.

Subtask B: Technical Marketing

Government Point of Contact: 

The Publications-Media team provides outreach products to promote the activities of the NAS Division and High-End Computing Capability (HECC) Project, and the science made possible by the Division's resources to the Center, agency, and the general public, as well as providing up-to-date technical documentation for the HECC user community.

Supercomputing Conference (Annually-Ongoing)

Produce and present content to general public and supercomputing community, highlighting work being done on agency supercomputing resources.

- Project Management
- Graphic Design and Printing
- Writing/Editing

Reporting

Supporting Division management by producing, editing, and compiling information and visual media for various reports throughout the year.

- HECC Monthly report (Monthly)
- Edit TN weekly highlights (weekly/as identified by management)
- SCAP Quarterly report (Quarterly)
- Pubs-Media team weekly report (Weekly)
- Other reports, as requested

Promotional Material, Marketing and Website Content

Creating outreach materials for the promotion of HECC resources and Division activities; promoting work done by users on HECC systems to public and media, maintaining technical documentation and notifications for HECC users, and providing content updates for websites.

- Create feature stories for NAS website (Monthly), news items for NAS website (as identified), and develop press releases for NAS/HECC announcements (as identified)
- Create/update/edit Knowledge Base articles, including continual improvement to articles and KB organization (ongoing/as needed), and write/edit System User Communications (as needed/identified)
- Record and post meeting minutes for HECC telecon (Weekly)
- Update and maintain AMS seminar pages on NAS website (Weekly)
- Provide general content/updates for NAS/HECC websites (as needed/identified) and program/project content (as identified/requested by project team/management)
- Provide web graphics (as requested/as needed), animations (as requested by management), and printed materials (semi-annually/as needed)
- Provide assistance to Division management's presentations, such as collecting media and compiling information from other sources (as requested)
- Media Relations – coordinated with Ames and HQ PAO and outside press
- Develop content for social media accounts (as identified)

Building/Tour Support

Supporting the Division by creating and maintaining building signage and displays in order to promote the HECC environment and history, assisting with large and VIP tours, and coordinating events and tours hosted by Ames PAO.

- Photography/Video: Tour photos/photography support for VIPs (as requested)
- NAS Building Support: Create new signage/building graphics (as requested); Update other building graphics (annually/as needed); Update HECC barometer poster (annually/as needed)
- Event Support: Create/edit content and provide staff for Ames Center events (as needed), Support Ames PAO staff during events in the facility, including requests to film/interview (as requested)

Other Tasks/Requests

- Edit documents: [REDACTED] requested by Division Management (as requested/needed)

Subtask C: IT Security for NAS Domain

Government Point of Contact: [REDACTED]

The contractor shall provide NAS with the following information technology (IT) security capabilities and services.

1. Maintain and enhance the NAS Situational Assessment System (NSAS) to provide the ability to detect and alert on security events that could impact the security of NAS systems and for which NAS needs to take action.
 - a. Advanced work shall include the following:
 - Detection of back doors that could be used by advanced persistent threats (APTs) or others to gain and maintain unauthorized access to NAS systems.

- Detection of APTs or externally planted code that is resident in NAS systems and communicating to external, hostile controllers.
 - Persistent attacks from a single actor that warrants the blocking of this attack site as well as related sites from the same organization.
 - Detection of possible shared accounts
 - Detection of misconfiguration of NAS systems that could open NAS to a successful attack.
 - Record progress and update as necessary to reflect new events, the table in the Security Event Appendix.
- b. The contractor shall store at least four months of flow, IDS, DNS, vulnerability scan, and log information to support the search for suspicious activity and the investigation of security incidents.
- c. The contractor shall assist government personnel in the development of a document that describes the design and implementation of the various components of NSAS.
2. As needed, make necessary modification to the weekly patch and vulnerability reports to correct known deficiencies, provide an accurate indication of the patch and vulnerability status of NAS systems and enhance the reports as necessary to help the administrators understand what needs to be done.
 3. Continuously assess the security state of NAS systems to identify threats and vulnerabilities, and then work with administrators to mitigate such threats and vulnerabilities.
 4. Perform work to ensure that NAS remains compliant with all security requirements applicable to NASA IT systems and uses best security practices.
 5. Perform any necessary incident investigations.
 6. Provide security consulting to the division and other areas of NASA as required. This also includes the review of proposed NASA regulations and participation in reviews of NASA projects as required.
 7. Perform operation and maintenance of NAS security systems.
 8. Work to transition responsibility for the upgrade, maintenance and operation of the Special Access system to other NAS groups that regularly develop and maintain support tools, but continue to support the system until it is transitioned.

Subtask D: Engineering Servers and Services

Government Point of Contact: 

The contractor shall:

Provide LSA (Lead System Administrator) system and user support for Mac OS and Linux desktop systems for NAS users. This includes new system deployments, regular OS and security patching, OS upgrades, backups, general application support and hardware maintenance. There are currently 303 TN user systems (102 Linux and 201 Macs); 114 TN servers (104 Linux – including 31 VMs; 8 Macs; and 2 Windows) and 21 group printers that

will be supported. It is expected that new technologies will be evaluated and may become supported systems during the year.

Provide LSA system and user support for Unix computer services such as printing (including printers and print servers), file servers, backups, email, patching, web servers, CVS, FTP, trouble ticketing, databases, account management and system administrative services, as well as OS support for servers utilized by other groups for their services. This includes regular OS and security patching, OS upgrades and hardware maintenance and upgrades. All services will be run on Linux or Mac OS.

Ensure user population, system counts, operating systems and server details are documented and up to date. Support for these systems includes:

- Provide 8x5 POC (point of contact) support for desktops and servers and 24x7 support for identified critical services.
- Provide web support as necessary to maintain ESS tools and ESS wiki web sites
- Provide development of automated tools and services to enhance the mobile computing model used for laptops.
- Monthly and critical patching for Red Hat 6, Red Hat 7, Yosemite, El Capitan, and Windows server
- Ongoing support for 201 Macs, 102 Linux workstations, and 114 servers
- Resolving user support Remedy tickets
- Identification of supplies, maintenance, hardware and software that needs to be procured for ESS projects
- Loaner system deployments
- Support Facility Shutdowns and Outages
- Support NS4 Security Plan testing and updates

Additionally, the contractor shall perform the following projects to the extent that efficient utilization of available ESS resources allow:

- Mac OS (Currently OS X 10.11 El Capitan) upgrade for Macs (about 210 systems)
- Red Hat 7 upgrade for Linux Workstations and Servers (about 215 systems)
- Completion and maintenance of Centrify PIV Authentication for Macs
- CFEngine 3 module upgrades for El Capitan OS
- Securing Macs: fix for port security
- Mac Refreshes for systems over 3 years old, and Linux Workstation refreshes for systems over 4 years old

- Take over SFE support from Security (OS and hardware support)
- Take over Radius support from Security (OS, hardware and application support)
- Take over support for the mini Hyperwall from Vis (OS and hardware support)
- Roll out Office 2016
- Refresh old servers (ESS, Networks, Tools, etc.) as needed
- Develop and roll out new Apple MacOS image after release of next version
- Identify and specify all the hardware, software and maintenance needed to accomplish these tasks

Subtask E: NAS Internal LAN

Government Point of Contact: [REDACTED]

Under this subtask the contractor shall perform network engineering, integration, testing, deployment, logistics and performance studies for the NAS LAN (NASLAN).

The contractor shall provide 24x7 POC (point of contact) support for LAN routers and switches.

The contractor shall provide EP-qualified (Elevated Privileges) network support for Cisco equipment within NAS Engineering Workstation and Server LAN. This includes new system deployments, regular IOS and security patching, IOS upgrades backups and hardware maintenance.

The contractor shall provide planning and coordination for proposed wiring upgrades in the office areas to support the upcoming Center-wide VOIP (Voice Over IP) telephone upgrade. In "Pod" areas where wiring is being upgraded, the contractor shall plan for incremental upgrades such as new Cat-6/6A wiring. All new wiring and upgrades are subject to funding availability. The VOIP system will be logically located on the ARCLAN network, but, in areas where the VOIP system is installed, layer-1 (physical wiring) maintenance will be supported.

Subtask F: Facilities (Building, Physical Security, Property Management)

Government Point of Contact: [REDACTED]

Facilities and Plant Engineering manages the complex subsystems of the physical computing facility. The contractor shall ensure all associated safety codes are met and provide engineering solutions to meet the expanding needs of the system. Additionally, the contractor shall handle the facility protection system to limit and control access to the facility.

The contractor shall provide property management in adherence to federal regulations and moving of all equipment and related items within the facility as well as in and out of the facility with NASA Property Management Systems (NEMS and IAM) and by NASA Property Management policy for shipping and receiving, excess equipment, and periodic reporting.

II Milestones/Metrics/Deliverables

No.	Milestone	Metrics	Deliverables	Date
PM1	Deliver CDRLs as specified in contract.	100%.	CDRLs	monthly
PM2	Track contract improvement & open issues.	1) Open improvements. 2) Open RCAs 3) Variance from schedule	1) Process improvement evidence 2) Completed RCAs	ongoing

Table 1 Program Management

No.	Milestone	Metrics	Deliverables	Date
TM1	Provide SC Conference and Special Events Support	Provide logistics and publication/multimedia products for the SC conference or any special events, as requested	1) Required handout materials, signage, and media coordination 2) On-site support 3) Lessons learned document outlining work completed and suggestions for improving future events	November 2016; as requested Document 2 weeks after event
TM2	Support Generation of Division/HECC Reports	Provide accurate, correctly formatted highlights, news, and publication slides covering all relevant material	Set of PowerPoint slides or other documents, as requested	5 th of each month; as requested
TM3	Provide Promotional Material, Marketing, and Website Content	Provide promotional material, animations, marketing, website content	Animations, marketing materials, website content, as requested	As requested
TM4	Building/Tour Support	Create photos, diagrams, and posters for the NAS Division	Documents/materials, as requested	As requested

Table 2 Technical Marketing

No.	Milestone	Metrics	Deliverables	Date
SE-1	Provide Enhancement to the NAS Situational Assessment System	Importance to NAS (High, Medium, Low), Actionable (nature of action that would be taken)	A demonstration of new operational capabilities as they become available	As needed
SE-2	Work with government personnel in documenting design of system.	Usefulness of the support.	Written and verbal responses to questions about the nature of the system.	As needed

No.	Milestone	Metrics	Deliverables	Date
SE-3	Patch and Vulnerability reports	Regularity of the report generation and accuracy of the information provided	Vulnerability reports tailored for each of the NAS support groups.	Weekly
SE-4	Provide Enhancements to the weekly patch and vulnerability reports.	Completeness and accuracy of the information in the reports.	A demonstration of new operational capabilities as they become available	As needed
SE-5	Notify appropriate NAS personnel and, as necessary, take action to mitigate security incidents and threats that are identified through the NAS Situation Assessment System or from outside of NAS.	Meets NASA regulations for timeliness for reporting incidents and mitigating threats.	Notice in the most appropriate form - phone call, email, or personal visit and timely mitigation of any threats.	As needed
SE-6	Delivery of security operational support to NAS to include the following: a. Direction and support to NAS system administrators to identify and correct security problems identified through weekly scan and vulnerability reports, console checks or code reviews, b. Internal and external consulting as required. c. Special access processing of requests and periodic password changes should be supported until these are transitioned to another group.	Meets NAS and NASA requirements for timeliness of support.	Security directions and help to NAS system administrators and NAS managers.	As needed
SE-7	Provide necessary documentation and leadership to ensure ongoing compliance with NASA security requirements including the following: a. Yearly support for independent security assessor in assessing the NIST SP 800-53 controls as required by NASA, b. Yearly Contingency Plan updates, training and testing. 	Meets NASA, ARC or NAS deadlines	a. Updates to Contingency Plan, along with Contingency Plan training material, and report on results of Contingency Plan tests b. Delivery of review, update or document as required	As required by ARC security

No.	Milestone	Metrics	Deliverables	Date
SE-8	Operation, maintenance, and upgrade of those systems for which NAS Security has maintenance responsibility, as well as security oversight for perimeter systems that may be maintained by other groups.	Security system downtime minimizes any downtime to NAS high end computing operations.	Problem fixes, patching and upgrades as required.	As required

Table 3 IT Security for NAS

No.	Milestone	Metrics	Deliverables	Date
ES1	Provide routine LSA support for NAS user systems and servers. Support new system deployments, OS and security patching, backups, general application support and hardware maintenance.	Timeliness of new system deployments, regular OS and security patching, backups, general application support and hardware maintenance.	Schedules or continuous support for NAS user systems and servers according to ESS Service Level support practices.	Ongoing. Report progress and issues monthly
ES2	Perform major upgrade work on each primary OS during the FY.	Completion of major upgrades on OS's supported by the ESS Group.	1) Complete upgrade of Mac OS systems to the latest version, El Capitan. 2) Develop Red Hat 7 image and initiate upgrade of Linux servers and workstations to Red Hat 7.	Ongoing. Report progress or issues monthly
ES3	Upgrade/refresh servers and personal systems, as required.	Completion of Refresh/Replacement of servers and personal systems scheduled to receive new hardware	Transition servers and personal systems to new hardware, when required	Ongoing. Report progress or issues monthly
ES4	Complete New Projects	Planning and completion of New Projects within the scope of ESS planned activities, optimizing the use of available ESS resources.	Completion of the Projects undertaken and documented in the NS3 Monthly	Ongoing. Report progress or issues monthly
ES5	Identification of supplies, maintenance, hardware and software for ESS projects	Timeliness of identification of items for ESS projects	Follow up on status of ESS procured supplies, maintenance, hardware and software with considerations for Government policies and practices.	Quarterly updates on status of ESS projects to the Government POC

Table 4 Engineering Servers and Services

No.	Outcome/Milestone	Deliverables	Metrics	Date
NT1	Complete network modifications in timely manner	Summary in NS3 monthly technical report	Time from request to connection (80% within 1 business day) & number of changes per month	Ongoing
NT2	Perform re-work/upgrades of LAN switch deployments using Catalyst 6800 switches as available	Routers/switches upgraded	Project completed on schedule and within budget. Completion date contingent upon availability of facility downtime.	April 2017
NT3	Plan for upgrading bandwidth from the NAS border through the core routers to the enclave border and to the enclave core to at least 40 Gbps total bandwidth, using either multiple 10 GbE or 40 GbE	Plan for upgrading to 40 Gbps aggregate bandwidth from border router through cores to enclave	Plan completed March 2016. Upgrade contingent on funding availability, including necessary network taps and upgrades to support NAS Security, the NASA SOC, and the DHS TIC monitoring.	Feb 2017
NT4	Coordinate completion of at least one Pod area upgrade, pending funding availability	Wiring installed and transition completed	Completed on schedule, prior to VOIP installation, contingent on funding availability	TBD

Table 5 NAS Internal LAN

No.	Milestone	Metrics	Deliverables	Date
FA1	Perform safety checks throughout the HECC facilities	NASA safety inspections turn up no category.	Monthly walk-through to check for and correct safety issues such as fire extinguisher checks, seismic bracing, safe storage, clear hallways, safe powering of electrical gear, etc.	Ongoing
FA2	Perform periodic scans of tagged equipment	Scan all equipment annually	Quarterly scans of tagged equipment and resolution of equipment not found during the scan	Ongoing

Table 6 Facilities

III Metrics

In each subtask area the contractor will work with the government POC and Task Requester to establish metrics. These will establish a means that the contractor can measure success on their near and long term goals. It is important that the contractor staff selects metrics and that they will aid in improving the product and/or services provided by the group. The initial list of metrics will be provided along with the deliverables and milestones in the Task Plan.. Modifications to the metrics can be made during the year with POC approval, but must be documented with the COR and a copy provided to the NASA CO.

IV Documentation and Reporting Requirements

The contractor shall:

- Discuss the monthly progress with the Task Requester.
- Schedule and conduct periodic task reviews after coordinating with the Task Requester, COTR and CO.
- Support in-depth presentations as scheduled by the Task Requester.
- Provide an electronic copy of the NF 533 for this task.
- Provide an electronic copy of the Monthly Technical Progress Report detailing the activity associated with this task, a summary of accomplishments, any problem areas and proposed action plans, and any issues by the 5th working day of the month.

V Travel Requirements

The contractor is expected to travel as required as necessary to perform this task. Travel will include:

- Attend training and conferences as needed to support this task.
- Travel to other centers as required.
- Attend technical meetings as required.

The Contractor shall provide to the Task Requester and Contract Management a Trip Report for both domestic and foreign travel that includes:

- Name of Traveller
- Trip Itinerary
- Task Name and Number
- Purpose of Trip
- Contact(s) and Summary of Discussion(s)
- Summary of Presentation(s) / Talk(s)

The following information shall be included in all Trip Reports for foreign travel:

- Statement of and Date of Threat Vulnerability Briefing
- Statement of and Date of Threat Vulnerability Debriefing (including the date the debriefing questionnaire was mailed to the Threat Vulnerability office. If no formal debriefing was required, so state)
- Statement of and Date of Export Compliance Briefing (if not applicable, so state and provide date of approval for 1676 package)

VI Government Property

The Government will furnish equipment (workstations, offices) as required for the successful completion of the task's requirements. All requests for new equipment will go through the appropriate POC.

VII Ames Management System Requirements

Work on this task shall comply with NASA Management System Policy - NPD1280.1, NASA Policies & Procedures - NODIS, Ames Management System Directives (APR1280.1), AMS Core Processes: APR7100.1, APR8060.1, APR8800.7; AMS Elements APR1220.1, APR1410.1, APR1440.1, APR8700.3, APR8700.2, and CDMS (see <http://ams.arc.nasa.gov>).

In addition, this work should comply with Ames Management Objectives (MO), for Code TN, specifically:

a. Center Level MO 1

Promote and maintain an organizational culture in which safety is paramount.

b. Center Level MO 2

Deliver key technical contributions to Agency-critical programs and projects, meeting all cost and schedule commitments.

c. Center Level MO 3

Produce outstanding research.

d. Center Level MO 4

Continually improve Ames Research Center processes.

e. Center Level MO 5

Develop and maintain a highly skilled workforce.

f. Continuous Improvement

Use the Center's Continuous Improvement Actions system.

VIII Security Requirements

Work on this task shall comply with the NAS Security Model and applicable U.S. Federal Government and NASA Policies and Regulations. In particular, work on this task shall comply with NPG 2810.1A and OMB Circular A-130.

IX IT Purchasing Requirements

Acquisition of IT products and services required for this task shall comply with applicable NASA IT procurement policies including the ARC CIO's IT purchase approval process (when required), Internet Protocol version 6 (IPv6) compliance policy and other requirements stipulated in NASA Form NF 1707.

X Other Requirements

Evaluation of Contractor's Response to SOR - Evaluation criteria of task proposal will be based on sound innovative technical approach, completeness of analysis, review and designs, proposed expertise and skill mix, and cost/price.

Award Fee Evaluation - Performance evaluation will be measured based on cost containment, quality of technical and status reports, adherence to metrics, and accomplishment of milestones/deliverables.

Task requires contractor access to Government database(s)? YES

NEMS—Asset Management System

XI Section 508 Requirements

Certain subsystem elements are expected to result in spreadsheets or databases that contain a substantial amount of information. This information and its presentation mechanism are subject to Section 508 of the Rehabilitation Act, Electronic and Information Technology (EIT) Accessibility. Complete information on EIT accessibility and Section 508, is available via Internet at <http://www.section508.gov>.

Specifically, the Contractor must propose EIT products and/or services that meet the applicable accessibility standards identified below:

- 36 CFR 1194.41 - Information, documentation and support

XII Quality Assurance Standards

The contractor shall be in compliance with all applicable NASA and Center-level Quality Assurance Standards and safety practices and guidelines.

XIII Appendices

Security Event Appendix

This appendix includes an initial list of the security events that are to be monitored and reported on. The contractor in consultation with the government shall add, delete or modify those events as necessary to improve the security of NAS. If the monitoring capability for the events shown in the appendix does not currently exist, then the contractor shall develop this capability. The following is the initial list organized by category and identified with an event identifier:

- Detection of externally exploitable vulnerabilities or attacks by outsiders
 - Attempted or successful attack
 - O-A-1: Focused attack on specific NAS SSH systems. The desire is to mark an attack as a hostile activity and then correlate this with other activities to see what else the attacker is doing in order to determine if this needs to be escalated to a high level of concern and action such as Tier 1 or Tier 2.
 - O-A-2: Focused attack on specific NAS Apache and web applications including, but not limited to buffer overflow, cross-site scripting (XSS), URI Chunk encoding, and PHP vulnerabilities in our NAS code
 - O-A-3: Specific IDS events of interest: look for pattern of same source, multiple rules
 - O-A-4: Specific IDS events of interest: DNS spoofing
 - O-A-5: Secure ID failure by IP address, which may be achievable even without getting this information from the Agency Two-Factor Token Infrastructure project that currently handles the actual SecurID authentication, since NAS can detect a failure to authenticate.
 - O-A-6: Failed password over a number of accounts. Initially this should just be looked at for the border systems.
 - Attacker use of back door
 - O-B-1: (also categorized as I-A-2): High order port becomes backdoor into NAS or Enclave
 - Indication of compromise
 - O-C-1: Specific events of interest coming from or going to a blacklisted site. If this is other than an IG request, then shall to correlate with other

- events, as appropriate, to see if this needs to be escalated to Tier 2 or Tier 1 for NAS security attention.
- O-C-2: Specific IDS events of interest: malware. NAS can see only that malware that we know about. SOC has more sources of possible malware than does NAS. Contractor shall work to get SOC list daily.
- O-C-3: Data flowing to sink hole.
- Vulnerability that could be subjected to external exploitation
 - O-V-1: Detecting vulnerabilities due to misconfiguration that could allow a break-in into the enclave. Contractor shall identify specific events to be monitored.
 - O-V-2: Detecting vulnerabilities due to ACL settings differing from what is required to minimize access to Enclave-resident systems. Security shall develop a list of unacceptable flows that can be used to check actual flows e.g., ssh traffic from outside going to Enclave resident system other than SFE.
 - O-V-3: Snort identified vulnerabilities -- initially put into Tier 3, but then move to Tier 1 or Tier 4 (in which case the particular rule for that vulnerability would be removed since the data is still held by Snort IDS). Need to remove rules from Snort so that only the events of interest to NAS are flagged.
 - O-V-4: Specific IDS events of interest such as web server listening on the wrong port. This should be Tier 1 or Tier 2.
 - O-V-5: Specific IDS events of interest, with metrics for management. In addition if there is a spike in the trends for the metrics, then this needs to be looked at more closely to see if it indicates something of significant concern.
- Data leakage including security events
 - O-L-1: Connection established between NAS and hostile IP address.
 - O-L-2: Foreign flow going to high order ports.
 - O-L-3: Monitoring for implanted Trojan horse code that is leaking information to a hostile location.
- Denial of service including security event
 - O-S-1: Extensive DOS or DDOS attack. While networks may address this, contractor needs to ensure that security knows about it.
- Detection of attacks or unauthorized use by insiders
 - Abuses by insiders
 - I-A-1: User system becomes supernode.
 - I-A-2 (also listed under O-B-1): High order port becomes backdoor into NAS or Enclave.
 - I-A-3: Contractor shall create a login profile for what is expected from each user. This should include information such as IP address from which they log in, time of day when they logged in, and duration of connection. This information can be used to discover deviations that could be used to detect various security issues including the following: a) from login-to-login look for differences in IP address and time-of-day as indication of possible account sharing. b) monitor for long-duration connections that are not associated with a running job to see if users are staying logged on even though they do not have a long-duration job running. c) monitor to see if users are logging in from designated countries as well as identifying all foreign log ins, which can be checked for legitimacy. Contractor shall begin with bastions and perform

analysis in syslog. If successful, then move to ESM or Portal. This may have a high false positive rate, so contractor needs to experiment with this.

- I-A-4: Execution of software that may be exploitable for unauthorized activity. This includes monitoring for activity on a port that has not been authorized for such activity. It also includes monitoring for unauthorized activity on a high numbered port greater than 1023. This will require that legitimate activity be defined.
- I-A-5: NAS users going to known malicious sites. What can be done for this is limited due to the fact that NAS does not do URL tracking, since the malicious site may have one URL, but multiple associated IP addresses. Also, currently NAS does not get any malware site information from the SOC. The contractor shall investigate and do what is possible. Note that traffic flowing to a NASA sinkhole provides some of this.
- I-A-6 (was I-A-8 on previous list): VPN connectivity to identify non-NASA or non-NAS machines that are connecting to NAS. This can be done using the syslog.
- Administrators not following rules
 - I-R-1: Monitor for users not using SU or SUDO to access root.
- Compliance
 - Logging
 - C-L-1: Identify hosts that are not logging to centralized log server.
 - Unauthorized services and flows
 - C-S-1: Monitor Flows to accomplish the following: a) verify that the ACLs have not been modified, allowing undesirable flows into NAS or the Enclave, b) verify that flows do not contain undesirable types of traffic such as telnet and ftp, c) verify that external traffic is not going to ports that violate NAS security policy, d) verify that mail is not going to somewhere other than the authorized mail servers, e) verify that correct traffic is going to expected hosts.
 - Assets
 - C-A-1: Detect new assets that show up in a flow, which are previously unknown and not in the host file. Eventually the contractor shall check hosts identified in flows against what the console check data shows.