

## PACE IV Core Work Area #1

Contains the following work areas:

- 31.00 Planning & Integration
- 34.00 Content Management & Collaboration
- 35.00 Enterprise Services
- 36.00 Multimedia Services
- 37.00 IT Security
- 37.01 IT Security Support for Code R
- 39.00 Customer Experience

### 31.00 Planning & Integration

#### **Agency Information Technology Architecture, Standards, Piloting and Services (SOW Reference 3.1)**

##### **Overall Objectives:**

The NASA Chief Information Officer (CIO) has responsibility for ensuring that NASA's information assets are acquired and managed consistent with Federal policies, procedures, and legislation, and that the Agency's Information Resources Management (IRM) strategy is in alignment with NASA's vision, mission and strategic goals. Information and information technologies are crucial to achieving NASA's strategic goals, and NASA's IT environment will transform to support and prepare for changes in NASA's mission activities.

The Emerging Technology and Desktop Standards (ETADS) group at the Glenn Research Center supports the NASA CIO in these endeavors, and specifically is responsible for developing Agency-wide desktop computing standards, providing an Agency mailing list service, and facilitating FISMA and HSPD-12 compliance. Systems expertise in the areas of architecture, standards, security, distributed systems, interoperability, virtual computing, collaboration, and others, will be applied to Agency wide efforts aimed at enabling NASA's mission, enabling integration of business (mission) processes and information across organizational boundaries, achieving efficiencies and ensuring that IT is efficiently implemented, and implementing and sustaining secure IT solutions.

##### **General Elements:**

The Contractor shall provide design, architecture, and piloting expertise to NASA in support of the NASA CIO. This includes:

1. Development and maintenance of NASA's hardware and software interoperability standards

2. Support of a production Agency mailing list service to facilitate discussions regarding the standards and other pertinent issues
3. Identification and testing of new and emerging technologies
4. Facilitation of NASA compliance with the Federal Information Systems Management Act (FISMA) by providing assessments, recommendations, processes, and procedures for secure operating system configuration
5. Facilitation of NASA compliance with Homeland Security Presidential Directive 12 by providing investigation, integration, and interoperability testing necessary to ensure that selected infrastructure and components for end user devices (smartcard readers, smartcard middleware, device drivers, public key infrastructure clients, system configurations, etc.) are integrated into the NASA desktop and end user device computing environment.
6. Documentation, advertisement, and promotion of workgroup standards and pilots as established by the NASA CIO and ETADS.

### **Capital Planning and Investment Control (CPIC) Support (SOW Reference 3.1.1)**

#### **Overall Objectives:**

Ensure compliance with OMB Circular A-11 (Specifically Section 53 and 300). Supports the GRC IT Investment Management process is to ensure accuracy and consistency in meeting the investment management and reporting requirements. Serve as the IT Approver in SAP, ESD and perform bankcard auditing in support of governance of IT investments at GRC.

#### **Specific Work Requirements:**

##### **CPIC Support:**

1. Upholds the CPIC framework and processes to ensure compliance and completion of Federal, Agency and Center requirements. Assesses framework to ensure correct level of effort, and supports development to continue to integrate and define supporting resources and appropriate improvements to strengthen and bring success to the framework.
2. Serves as an agent to support integration of the identified IT Disciplines, as well as with the Center Office Chief Financial Officer and Agency efforts. Effort leads to a stronger collaborative framework, to aid in understanding.
3. Ensure completion of all Major and Non-Major Center IT Investments. Coordinates with IT Investment Owners in providing aid in completing the reporting requirements, and leads kick-off and guidance development to sustain and facilitate activities.
4. Support Agency submission of OMB required Exhibit 53 and Exhibit 300 reports. Requires submission of all Center reporting requirements, as a finalized document and support assessments and review to ensure accuracy of both OMB requirements.
5. Sustain and provision Center IT Portfolio Management procedures and analysis. \*Leads package development to be reviewed by management, stakeholders and customers to properly assess and review current state. Coordinate with Enterprise Architect to additionally illustrate alignment of current state with identified future state.
6. Provides support in clearly identifying investments with the funding structure and supporting the integration of financial formulation and execution templates with the upkeep of the IT Investment and BY SIBC.

### **IT ESD Approvals (SOW Reference 3.1.1.4)**

The ESD IT Approver works closely with the ESD, NICS and ACES SME to ensure that technical requirements are aligned with the purchases being requested from I3P.

1. Check service request for adherence to IT policies
2. For APC purchases the link to the catalog is there and working
3. The correct service request was selected
4. Correct Org Approver was selected to fund the purchase (ex: users who are located in Code D but work on a Code M project)
5. Adequate justification is being provided as needed
6. Other requirements as defined by the SMEs
7. IT Bankcard Auditing:
8. Evaluate Bankcard purchases on a monthly basis for the IT charge codes for hardware, software and other purchases
9. Ensure purchases are in compliance with the processes and procedures defined by the Vendor Management Lead and GRC Procurement Office
10. Apply the IT Investment governance process to the purchasing of hardware and software using bankcards.

### **End Products:**

1. Ensure all required data is entered into the Agency Exhibit 53 and 300 tool in alignment with the Agency PPBE schedule.
2. All IT SAP PR, ESD Approvals and Bankcard audits shall be processed in the appropriate system (ESD, Bankcard, SAP)
3. Apply the CIO defined governance process to IT Investment management as specified by the Integration Division and Business Manager

### **IT SAP Approver (SOW Reference 3.1.1.4)**

1. GRC IT PR Approver: Review, verify and approve IT PRs on a daily basis.
  - a. Verify Material Group Numbers are correct for each line item; if this number is not correct, notify the requisitioner and notate in the header within SAP (If action to correct the Material Group Number is not taken, the PR may be rejected.)
  - b. Verify that NASA C-962 form (Mobile Devices Request for Waiver) is attached to the PR and properly completed in SAP, for all mobile device purchases.
2. Verify that PRs with a special request/waiver have NASA Form 1707 (Special Approvals and Affirmations of Requisitions) is attached to the PR and Part 8 is filled out correctly.
  - a. Coordinate with OCIO IT Service Owners to obtain their approvals, as needed, for specified purchases. Do not approve PR until the OCIO IT Service Owner discusses the purchase with the requestor. Notify requestor of this action by (1) documenting action taken in the SAP header and (2) through email or telephone call. Follow-up with the OCIO IT Service Owner regarding the resolution. The OCIO IT Service Owner will contact the requisitioner or the individual who requested the purchase.
  - b. Ensure the product/service being ordered is not attainable through the ACES contract.
  - c. Log, aggregate, and mine the IT PR data for cost/resource efficiencies Mine data from SAP data base, prepare PowerPoint slides for and attend monthly OCIO Business Review, providing charts showing monthly distribution of categories, items ordered, purchases per organization and other data as requested. Provide copies of

- results to the Business Manager and Vendor Management Lead at least one day prior to the Business Review or as requested.
- d. Review each Directorate's Strategic Investment Business Case (SIBC) on a regular basis and verifies IT PR requests and Bank Card purchases align with the respective SIBC.
3. Notify OCIO's Leadership Team, Mission Specialists, Vendor Management Lead, key OCIO IT Service Owners and Relationship Managers of anomalies.
    - a. Recommend improvements to the IT PR approval process to the Business Manager and Vendor Management Lead.
    - b. Work with GRC Procurement POC and GRC Financial Office POC to ensure data is being collected properly.
    - c. Provide and train a backup. IT PRs shall not remain in the SAP queue more than two business days without some type of action taken.
    - d. Provide SAP data and analyze for cost/resource efficiencies. The OCIO Vendor Management Lead may request data on a regular or ad hoc basis, as determined by the Vendor Management Lead's needs and requirements.

### **OCIO Program Management Support (SOW Reference 3.1.2)**

#### **Summary:**

A full range of program management support services will be provided to the OCIO under this work area. These include but are not limited to Configuration Management (CM), Project Portfolio (PP), Project Management (PM), and Service Portfolio (SP) processes. Definition and automation of a subset of code V configuration items for each process area (CM, PP, PM, and SP).

### **Agency Information Technology Architecture, Standards, Piloting and Services (SOW Reference 3.1.3.2 and 3.1.3.3)**

#### **Overall Objectives:**

Desktop Computing Standards (DCS) - Develop and Maintain NASA-STD 2804, Minimum Interoperability Software Suite and NASA-STD-2805, Minimum Hardware Requirements

#### **Deliverables:**

Support one major and one minor update to these standards with requisite research and testing. Develop, review and/or maintain supporting guidelines, websites and whitepapers. Maintain and support a production Agency Mailing List Service (AMLS) for the purpose of facilitating communications and discussions revolving around the technologies included in the Standards. Assist in the development of NASA operation procedures, policies, and guidelines as required.

### **Testbed Maintenance: Maintain the ETADS Testbed, the "Emerging Technology Assessment Facility" (ETAF), and Associated Services (SOW Reference 3.1.4)**

#### **Overall Objectives:**

Support necessary system configuration, application testing, and network services, to ensure that ETADS group recommendations and other Agency efforts are based on sound technical solutions. Identify opportunities for improving the testbed environment. Ensure availability of the

testbed for evaluating and testing the integration of services into the NASA environment. Develop and Maintain IT Security Plans and Risk Assessments for all testbed systems. Provide expertise in Microsoft Windows technologies, especially as they relate to providing enterprise-wide solutions. Participate in key Agency working group.

**Deliverables:**

As requested, provide a presence at critical Agency working groups that align with the goals of ETADS by consulting, attending teleconferences and face-to-face meetings as necessary, monitoring mailing lists and discussion forums, reviewing documents and completing other action items as required.

**Agency Security Configuration Standards (SOW Reference 3.1.4)**

**Overall Objectives:**

Lead the NASA Agency Security Configuration Standards (ASCS) Project to ensure NASA compliance with system configuration requirements of the Federal Information Systems Management Act (FISMA); develop Agency Security Baselines derived from the National Institute of Standards and Technology (NIST) Federal Desktop Core Configurations (FDCC), United States Government Computing Baseline (USGCB), the Center for Internet Security (CIS) Benchmarks, or other acknowledged sources of security configuration standards. Provide organizational support for a forum, records, and Center Points-of-Contact interactions which ensure operational requirements to modify security baselines are surfaced, evaluated, tracked, and recorded. Provide an organizational process for the incorporation of emerging IT security threat information into Agency security baselines. Evaluate, establish and maintain processes for implementation, and facilitate deployment and auditing of, Security Configuration Baselines for NASA; Maintain NASA Membership in the CIS.

**Deliverables:**

Assist with related Agency IT Security initiatives and incorporate security into ETADS standards and other deliverables. Provide Agency level management of security baseline alteration records. Provide periodic summary reporting of Agency compliance status. Assist in the development of Agency compliance reports, as required.

**Desktop Smartcard Integration (DSI) and Identity, Credential, and Access Management Engineering (ICAM) Support (SOW Reference 3.1.4)**

**Overall Objectives:**

Ongoing sustaining engineering for Desktop Smartcard Integration (DSI) installer packages; maintain the standards associated with smartcards and smartcard readers; maintain the configuration guidelines to enable end user device interoperability with the ICAM Infrastructure, including trust anchor management and enhancements to the NASA smartcard; perform new technology assessment and pilot activities for possible incorporation into the end user device environment and device standards; provide ICAM sustaining engineering and technical support information to NASA application and service providers for the integration of NASA systems with

existing components of the ICAM Infrastructure; advise on recommendations to the overall ICAM Architecture.

### **Specific Work Requirements**

**Desktop Computing Standards (DCS)** - Develop and Maintain NASA-STD 2804, Minimum Interoperability Software Suite and NASA-STD-2805, Minimum Hardware Requirements

#### **Deliverables:**

Support one major and one minor update to these standards with requisite research and testing. Develop, review and/or maintain supporting guidelines, websites and whitepapers.

### **Agency Security Configuration Standards (SOW Reference 3.1.4)**

#### **Overall Objectives:**

Lead the NASA Agency Security Configuration Standards (ASCS) Project to ensure NASA compliance with system configuration requirements of the Federal Information Systems Management Act (FISMA); develop Agency Security Baselines derived from the National Institute of Standards and Technology (NIST) Federal Desktop Core Configurations (FDCC), United States Government Computing Baseline (USGCB), the Center for Internet Security (CIS) Benchmarks, or other acknowledged sources of security configuration standards. Evaluate, establish and maintain processes for implementation, and facilitate deployment and auditing of, Security Configuration Baselines for NASA; Maintain NASA Membership in the CIS.

#### **Deliverables:**

Assist with related Agency IT Security initiatives and incorporate security into ETADS standards and other deliverables.

### **Messaging and Collaboration (SOW Reference 3.1.4)**

Continue to surface and evolve collaborative application requirements for team collaboration, research, test and pilot promising collaborative tools and environments (such as WebDAV, peer-to-peer, online awareness/instant messaging, video conferencing, team services, and others), and recommend architecture and standards for collaborative technology as needed.

#### **Deliverables:**

Continue to support and provide consultation to NASA's Operational Messaging and Directory Service (NOMAD) based on Exchange Server for electronic mail and calendaring.

### **ETADS Office Management (SOW Reference 3.1.4)**

In collaboration with the ETADS Program Manager, ensure the efficient operations of ETADS business functions. Track and maintain ETADS hardware, software, and services inventory. Initiate and track purchase requests and coordinate travel. Assist in tracking the Project Management actuals by creating phasing plans, tracking workforce data, and responding to data calls as required.

Additional Support Provide critical analysis of existing NASA IT services relative to their integration into the NASA infrastructure. Respond to ad-hoc requests for information and consulting to the Agency OCIO.

### **NASA IT Labs Projects (SOW Reference 3.1.4)**

**Overall Objectives:**

The purpose of this project is to provide support for developing and submitting IT Labs proposals.

**Specific Work Requirements:**

Support NASA IT Labs Projects

1. Identify and recommend potential projects for inclusion in IT Labs.
2. Support the development and submittal of IT Labs proposals.
3. Develop and manage IT Labs project schedules.
4. Provide status of project activities as requested, at a minimum bi-weekly.
5. Perform project activities, such as:
6. Product/technology research, assessment and evaluation
7. Integration of products with NASA IT infrastructure
8. Coordination of user testing
9. Compilation and presentation of test results
10. Creation and implementation of pilot projects
11. Development of pilot to production schedules and guidelines
12. Other activities, as requested
13. Develop project documentation and conduct presentations/out briefs as requested
14. White papers
15. Test results
16. Technical Position Papers
17. In briefs
18. Out briefs
19. Project Status Reports
20. Lessons Learned
21. Other documentation, as needed
22. In support of projects, act as liaison between NASA and hardware/software product vendors.
23. Provide and maintain IT infrastructure as required to support IT Labs project.
  - a. Identify dependencies on external or other NASA IT environments at project outset.
  - b. Install and maintain needed software and hardware.

**Service Management for the OCIO (SOW Reference 3.1.6)****Overall Objectives:**

Develop a comprehensive Service Asset & Configuration Management (SACM) system to maintain all GRC IT assets and configuration items to include desktops, laptops, monitors, plotters, printers, projectors, equipment racks, physical and virtual servers, tape and storage devices, network devices, radios, telecommunication devices, mobile devices, smart phones, software/applications, websites, documentation, etc. encompassing both the I3P and non-I3P infrastructures at Lewis Field, Plum Brook Station, and Center related offsite locations.

Incorporate updates from other data sources to ensure accuracy. These sources may include, but are not limited to, NPROF, KACE, Foundstone, Active Directory, ITSEC-EDW, IPAM, and I3P. Ensure the SACM database is kept current by establishing processes for applying updates and by inserting SACM database updates into existing processes (De-subscriptions, new ACES seats, Refresh, IT purchases by individual organizations, etc.).

Thoroughly document all processes. The SACM system shall be expandable to include new data elements as determined by the GRC Office of the Chief Information Officer (OCIO). This includes, but is not limited to, Data at Rest (DAR) encryption compliance. As the Agency standardizes on an authoritative Configuration Management Database (CMDB), coordinate with the End-User Service Office and reconcile the local SACM database with the authoritative CMDB.

Work with other service providers (ACES, NICS, etc.) to reconcile differences between their reported IT assets and configuration items and the information contained within the Center's SACM system. Provide web-based access to the SACM system for reporting purposes.

Coordinate SACM efforts with the Center's I3P Project Team, the GRC Enterprise Architect, and the GRC IT Configuration Manager.

**Phase 1:** To define requirements and a representative set of Configuration Items, projects, services and processes to be implemented for a Service Management System for the OCIO. Setup and maintain a common automated process for Configuration Management of OCIO services, Project Portfolio Management of OCIO projects, Project Management (WBS, schedule, etc.) and Service Portfolio Management (list of current and target state services).

**Phase 2:** To implement IT Service Management for the OCIO as specified in Phase I. Implementation to include acquisition of approved solution, system security plan, organizational change management, and configuration of the approved solution including representative use case/data entry. While the Phase II duration is six months, the objective is to deliver early value to the OCIO (e.g. implement Configuration Management in month three) per the implementation plan. Overall, at the end of Phase II, the OCIO will have a basic IT Service Management environment including adoption of OCIO staff and integration into the OCIO work processes.

### **Enterprise Architecture: Support Development of Agency Architecture (SOW Reference 3.5)**

#### **Overall Objectives:**

Maintain an awareness of and make contributions to the overall NASA IT Enterprise Architecture effort and participate as requested in support of the End User Domain architecture.

#### **Technology Maintenance and Exploration:**

Track current technologies such as desktop hardware and software (operating systems, applications), mobile devices, server based technologies, collaborative technologies, and Microsoft and open source solutions, through research and prototyping which can be leveraged to lower IT costs and improve Agency-wide interoperability and collaboration. Ensure that ETADS continues to be sought after as an Agency partner in the development and/or identification of new technology that targets improvements in interoperability and collaboration and identify emerging technology and trends that can be leveraged by the Agency.

#### **Deliverables:**

Maintain technical expertise through training, education, conference attendance, research, testing. Facilitate the transfer of knowledge and professional observations to NASA in the form of technical recommendations and consultation, white papers, web sites, standards.

Evaluate emerging technologies for their ability to integrate into the NASA environment. Recommend technologies that will maximize NASA's investment by having the greatest overall impact to the environment. Propose any necessary modifications to the environment to accommodate recommendations.

**Agency List Server Support (SOW Reference 3.5.2)**

Maintain and support a production Agency Mailing List Service (AMLS) which facilitates agency communications and discussions including those revolving around the technologies included in the Standards.

**34.00 Content Management & Collaboration**

**Advanced Engineering Collaborative Support (SOW Reference 3.4)**

**Summary:**

This work area provides collaborative room coordination and technical support for Advanced Engineering and Engineering Design Center Environments activities under the Agency's Engineering organizations.

**Advanced Engineering Collaborative Environment Design and Implementation Support (SOW Reference 3.4.1)**

**Description**

**Overall Objectives:**

This work area provides collaborative design and implementation support for Advanced Engineering and Engineering Design Center Environments under the Agency's Engineering organizations. The support required is focused on: gathering and documenting requirements from customers; understanding current collaborative technologies, systems, and capabilities; and designing new or enhanced collaborative capabilities in designated spaces to fulfill the customer's needs.

**Specific Work Requirements:**

This design or upgrade of collaborative facilities is on an as-needed basis. NASA customers who request this particular support must work with the Task Monitor to clarify the scope and funding for the effort prior to work being done by the contractor. Funding will be added to this particular work area for specific facilities, capabilities or upgrades as necessary.

The following list details the work performance elements that may be required depending on the scope of the particular design or upgrade:

1. Gather customer requirements for collaborative environment(s) and document them as appropriate. Gain a fundamental understanding of the customer's project and team as well as understand any pertinent resource constraints (funding, location).
2. Provide design or upgrade options to the customer along with rough order of magnitude (ROM) costs to assist in decision making.

3. Once design or upgrade choices are finalized, provide a detailed plan to include estimated costs (with quotes from sub-contractors), description of services required from Center contracts (e.g. - Call Henry), and a coordinated schedule encompassing all items.
4. Create/coordinate/assist in the procurements, purchase orders, or work orders/Infrastructure Upgrade Proposals (IUPs) necessary to accomplish the assigned tasking. Additionally, track and inventory all shipments, receivables and warranties/documentation.
5. Coordinate the scheduled activities (purchases, construction, etc.) such that the facility or upgrade is completed within the schedule allocated.

Conduct a final review of the facility or upgrade to verify successful completion.

Specific Work Items:

1. Provide estimate for Task Monitor approved collaborative upgrades or installations. [Will be listed here as they are requested and funded - currently none planned]

#### **End Products:**

Collaborative environments or upgrades to existing environments that meet the customer's cost, schedule, and performance requirements as agreed upon at project initiation and approval.

### **COMPASS and SCENIC Advanced Engineering Collaborative Environment Support (SOW Reference 3.4.1.1)**

#### **Description**

#### **Overall Objectives:**

This work area provides technical support for Advanced Engineering and Engineering Design Center Environments. In particular, this effort will support the COMPASS and SCENIC collaborative environments. The support required includes the following main categories: computer administration, computing/collaborative infrastructure integration/operation, and environment support of studies and requirements activities.

#### **Specific Work Requirements:**

Provide primary support for Computer Administration duties:

1. Installation of software
2. Management of collaboration room workstations, laptops and applications as necessary.
3. Workstation UserID and computer resources management
4. Development, implementation and maintenance of Computer Security Plans for COMPASS and SCENIC environments.
5. Support of procurements and system integration with other collaborative systems.
6. Computing/Collaborative infrastructure and integration duties:
7. Support of collaborative environments (video, audio, and data sharing) as needed by the customer.
8. Integration of Engineering tools for use by Engineering Design teams (network access, and platform interdependencies).
9. Support Security Plans, procurements, testing of new equipment, and technology planning.
10. Coordinate and schedule regular maintenance, new system integration, and equipment repair issues for the COMPASS and SCENIC environments.

11. User support to foster the utilization of the collaborative environments to their fullest potential.

**End Products:**

The facility will be supported in a day-to-day manner within the allocated resources to debug problems, integrate user requirements, and ensuring the smooth operation of the environment.

**Virtual Team Collaboration and Knowledge Management (SOW Reference 3.4.1.1)**

**Summary:**

This work area will provide support for acquiring, implementing, operating, and supporting the adoption of virtual team collaboration and knowledge management systems at NASA GRC. This work area will also provide support for the overall development of virtual team collaboration at NASA GRC including pilots and standards development.

Expertise in the areas of security, distributed systems, interoperability, collaboration, and adoption practices focused on enabling NASA GRC systems and interoperability with NASA external partners. Document, advertise, and promote workgroup standards, pilots, and services as established by the NASA GRC CIO.

**General Elements:**

Support the roll out of Knowledge Worker Infrastructure (KWI) services at NASA GRC to enable corporate collaboration, knowledge capture, knowledge leveraging, and continuous process improvement at the center. Perform implementation and administration; problem diagnosis and resolution; and upgrades and maintenance - for all components of the GRC KWI that may include: a virtual team space, a GRC repository via a document/content management service, and others.

Provide customer support for all GRC KWI services. Provide facilitation if necessary to teams to enable successful adoption of the applications. Provide application demonstrations and account administration as necessary.

Contribute to the advancement of GRC KWI services. Perform research, testing, standards development, support documentation (i.e., system architecture documentation, operational procedures, and user documentation, etc.), and operational planning as necessary. Also perform customer communications, website maintenance, acquisition of services, usage reporting, and attend training as necessary.

**Knowledge Worker Infrastructure (SOW Reference 3.4.1.1)**

**Description**

**Overall Objectives:**

The scope of this includes the following objective:

**Knowledge Worker Infrastructure**

This work area shall support existing and future collaboration tools in support of the Knowledge Worker Infrastructure (KWI) at NASA GRC. KWI enables corporate collaboration, knowledge

capture, knowledge leveraging, and continuous process improvement at the center. Goals include: continued excellent service to eRoom customers, maintenance of eRoom and all supporting software at vendor supported version levels, monitoring application resources proactively to avoid service disruptions or performance degradation, and planning for migration from eRoom to a new environment (Google Apps, Sharepoint, and other options to be considered).

**Objective 1:** Maintain an up-to-date, reliable, and secure eRoom system. Support software tools, policies, and procedures as they pertain to this system.

**Objective 2:** Coordinate the purchase, installation, customization and testing of eRoom software to maintain the product at supported release levels.

**Objective 3:** Rollout eRoom supplemental software and provide customer support for KWI tools.

**Objective 4:** Rollout and administration of YADA.

**Objective 5:** Testing/evaluation of emerging collaborative tools (Alfresco, SharePoint, Google Apps, Life Ray, Jive ...) deemed appropriate for the forward path of the KWI.

This work area also includes support of Agency initiatives as they are developed and implemented at GRC as agreed upon with the NASA GRC Technical Monitor (TM).

**General Work Requirements:**

1. Work Prioritization: All work including projects, major environment changes, upgrades and service enhancements are agreed to by and prioritized in conjunction with the TM.
2. Projects: A project is defined as a grouping of tasks to accomplish a specific goal. A project is not created because of any particular level of cost, hours, or scope. A project may be created for an item of management interest or because the TM has a need to track the specific tasks involved.
3. For project assignments assigned by the TM under this work area, project plans shall be developed within an agreed-upon timeframe. These plans, which will be maintained by the contractor, will contain, at a minimum:
  - a. Project schedule, including hours by work area
  - b. Major milestones within schedule
  - c. Estimated completion dates
  - d. Known project interfaces and dependencies
  - e. Test plan
4. Deliverable Deadlines: Project milestones and on-going tasks are expected to be completed on-time. Changes to due dates can only occur with approval of the TM.
5. Monthly Reports: Monthly reports will contain the following information:
  - a. Actual hours expended per significant Objective and Project.
  - b. Overview of activities performed during the month and recommendations for next month's activities
  - c. Data supporting each of the metrics. Quantity and format of the data shall be determined in conjunction with the TM.

6. Meeting Attendance: PACE will be represented at team meetings unless agreed to by the TM.
7. Documentation: Documentation requested by the TM shall be complete, accurate, and useful.
8. Procurements: Software purchases and licensing shall be coordinated with the TM.
9. Availability: All KWI applications shall be operational 24 x 7, excluding approved maintenance windows and other system outages
10. Software Version: Software will be at the current vendor's version within 6 months of release unless otherwise determined by the TM.
11. GRC Standards and Policies: Software changes and upgrades shall be implemented in accordance with GRC configuration management requirements and performed within GRC approved maintenance windows, unless an exception has been approved by the TM.

### **Specific Work Requirements:**

#### **Objective 1:**

Maintain an up-to-date, reliable, and secure eRoom system. Support software tools, policies, and procedures as they pertain to this system.

1. Provide ongoing operational including: site administration including configuration settings, testing and coordination of new software releases, and implementation of customizations on an as needed basis.
2. Develop and update all customer documentation needed to effectively utilize eRoom.
3. We will continue to re-provision customer data as necessary and we will, in the future, migrate customer data to the new storage arrays when the Hosting team makes them available – as required for improved performance.
4. Provide service problem identification and resolution including monitoring, problem diagnosis, and problem resolution in conjunction with appropriate providers (virtual team space service vendor, network, IT security, desktop, etc.). Provide monthly usage and additional capacity reporting as requested.
5. Incorporate evolving mechanisms for agency IT System user authorization and directory services as they become available.
6. Participate as necessary in the development and maintenance of security plans including risk assessment and contingency plans per NASA NPR 2810.1, as led by the Hosting work area.

#### **Objective 2:**

Coordinate the purchase, installation, customization and testing of eRoom software to be installed at GRC, including any upgrade releases.

1. Provide ongoing operational including: site administration including configuration settings, testing and coordination of new software releases and implementation of customizations on an as needed basis.
2. Develop and update all customer documentation needed to effectively utilize eRoom.
3. Provide service problem identification and resolution including monitoring, problem diagnosis, and problem resolution in conjunction with appropriate providers (virtual team space service vendor, network, IT security, desktop, etc.). Provide monthly usage and additional capacity reporting as requested.

**Objective 3:**

Rollout eRoom supplemental software and provide customer support for KWI tools.

1. Respond to all received customer inquiries, whether received via email, telephone, or face-to-face within 8 business hours of receipt.
2. Assist Civil Servant team members with customer inquiries as necessary.
3. Provide Help desk/User Support which will leverage vendor user support services and other existing help desk/user support mechanism provided through NASA contracted services including I3P and IMCC. This support service will be available from 8am – 5pm Monday through Friday. Manage accounts including adding, removing, and managing account information including passwords.
4. Provide customer support and team adoption functions including: customer communications (e.g., appropriate emails), new customer familiarization assistance, documentation and sharing of service best practices and FAQ, and development and maintenance of room and object templates.

**Objective 4:**

Installation, rollout and administration of YADA.

1. Ensure the functionality of the tool is working properly to enable access to eRoom data and objects after the transition from the eRoom tool.

**Objective 5:**

Testing/evaluation of emerging collaborative tools (Alfresco, SharePoint, Life Ray, Jive) deemed appropriate for the forward path of the KWI.

1. Install, test, and pilot future collaborative tools as deemed necessary by the TM.
2. Future collaborative tools include but are not limited to Alfresco Share, Microsoft SharePoint, Jive, Google Apps, and LifeRay Portal.

**Additional General Work Requirements:**

1. Security: Support security plan development and maintenance in coordination with the GRC IT Security Program office.
  - a. Implement security controls required to maintain authority to operate NIST Moderate level systems
  - b. Implement and enforce all NASA IT security policies
  - c. Attend security plan meetings, if requested by TM

- d. Provide input to security plan and supporting documentation
  - e. Support security audit and review activities
  - f. Address outstanding Certification and Accreditation POA&Ms, ensuring completion by required dates.
  - g. Apply all security-related software patches as required by GRC and NASA
  - h. Monitor systems, logs, and software configurations on a regular basis, as agreed upon by the TM
  - i. Provide support for application developers to properly secure applications and assist them in development of application related security documentation
2. Response Time: Normal requests by the TM or a customer are completed within 48 hours of receipt, unless otherwise determined by TM. Requests defined as urgent by the TM are completed within 24 hours of receipt.
  3. Hours of Coverage: We will provide Help desk/User Support which will leverage vendor user support services and other existing help desk/user support mechanism provided through NASA contracted services including I3P and IMCC. This support service will be available from 8am – 5pm Monday through Friday. We will manage accounts including adding, removing, and managing account information including passwords.

## 35.00 Enterprise Services

### **Enterprise Administration Support (SOW Reference 3.5)**

#### **Summary:**

Provide Enterprise Administration systems support for the following three work areas: ICAM, STRAW and Enterprise Systems support.

### **Enterprise Administration Support (SOW Reference 3.5.1)**

#### **Description**

#### **Overall Objectives:**

#### **Objective 1: ICAM Support**

The scope of this work area includes support for all NASA GRC ICAM, On-Boarding Process and IEMP activities.

#### **Objective 2: STRAW Support**

The scope of this work area includes support for the NASA System for Tracking and Registering Applications and Web sites (STRAW) activities.

**Objective 3: Enterprise Systems Support**

The scope of this work area includes support for the NASA Enterprise Directory (NED), Enterprise LDAP, and the NASA Data Center (NDC) account management activities.

This work area also includes support of Agency initiatives as they are developed and implemented at GRC as agreed upon with the NASA GRC Technical Monitor (TM).

**Specific Work Requirements:**

**Objective 1: ICAM SUPPORT**

1. Provide associate Center Logical Business Process Lead (aCBPL) support to GRC.
  - a. Perform provision, suspend, modify and de-provision requests.
  - b. Provide GRC IdMAX/NAMS User community assistance with submitting and researching NAMS requests.
  - c. Support NAMS activities, including participation in weekly telecons and workflow development, testing, and implementation.
  - d. Investigate Identity and Account management issues as requested.
2. Integrate latest IdMAX processes into On-Boarding account procedures. Keep Program Leads informed and provide updates to the Summer Staff website.
3. Respond to requests to research Domain and email access for new hires. If needed, investigate the cause and perform the appropriate action.
4. Perform IMART and custom ad-hoc reporting upon request.
5. Support information maintenance and assurance for all NAMS users interface related activities including IdMAX.
6. Support the Center's ICAM effort to migrate applications into NAMS (migrate approximately 4 applications per month)
  - a. Discuss the NAMS workflow with applications owners (i.e. conduct interviews)
  - b. Build (define) the applications using Resource Maintenance Tool (RMT)
  - c. Test in Sandbox (conduct testing)
  - d. Migrate application into Production
  - e. Grandfather existing accounts into NAMS
    - i. Gets user list from application owner
    - ii. Verifies the identity in NED obtains UUPIC
    - iii. Gets role information to match fields in the NAMS workflow
    - iv. Create properly formatted NAMS account records to load

**IEMP OPERATIONAL SUPPORT:**

1. Perform User Management functions as specified for each system, including the addition, modification and deletion of user accounts.
2. Perform role management as specified for each system including the addition, modification, and deletion of roles.
3. Perform password resets for all designated IEMP related systems (Core Financial, Business Warehouse)
4. Monitor monthly reports to address invalid logins.
5. Comply with audit reporting requests.
6. Coordinate separation of duties (role conflicts)
7. Coordinate with IEMP Change Management
8. Monitor the Admin Remedy Queue (s) in support of IEMP System security management and respond to user problems/requests identified therein.
9. Provide User Support during core and extended business hours.
10. Provide problem resolution.
11. Compile or forward NEACC generated reports for the semi-annual revalidation of all applications and coordinate the IEMP CBPL sign-off form to be fax`ed to the NEACC.

**Objective 2: STRAW CENTER ADMINSTRATOR (CA) SUPPORT**

1. Assist users with creation of new - website, web application and application registration.
2. Assist users with maintenance and changes to existing registrations.
3. Assist users with questions. The questions range from "how do I login," or "what needs to be registered," to walking them through the registration process.
4. Track the registration process and send reminder emails as needed.
  - a. Monitor the Management Approval queue and send out email reminders to approve the record. (normally it should be approved within 30 days)
5. Inform CA of issues or registration failures.
6. Periodically run reports for overdue records and send email reminders to Responsible NASA Official and Curator.
7. Update records in STRAW as requested, for example changing a registrant name.
8. Approve account request through NAMS and then create the account in STRAW.
9. Maintain external and internal distribution lists i.e. modify new/changed registrants and application owners on lists as appropriate.

- a. Create new list per request of CA.
- 10. Maintain the list in STRAW for Policy and Content points of contact.
- 11. Inform Web team of pending (within 30 day) Sec. 508 scan expirations.
- 12. Run reports per request of CA.

**Objective 3: ENTERPRISE SYSTEMS SUPPORT**

- 1. Monitor the daily transfer of data files between GRC and the NEACC. Conduct preventive maintenance, backup, and upgrades of the ICAM update (NED) process as needed.
- 2. Support GRC's DSA (Directory Services Application) database.
  - a. Monitor the updating of local directory information by 1) individual employees and administrators on their behalf, 2) mass move update requests, 3) the Security Office SIMS system, and 4) agency IdMax changes via the ICAM IDA files. Data changes include locator information, employee codes, 2-level User organizational mappings, User ID's, and other ICAM related information.
  - b. Apply local directory information changes to the legacy Enterprise Tables.
- 3. Extract agency LDAP data daily to allow for data distribution and Oracle database access to support various GRC application systems such as WADE, IRIS, HCIE, SIMS, and the Mail Room.
- 4. Monitor the daily transfer and update of EPayroll employee, transaction, transfers, and Organization table data into the local database environment.
- 5. Interact with the NEACC regarding ICAM issues such as: troubleshooting, planning for and implementing any proposed NED structure changes. Monitor daily operations including changes that need to be made to the local directory structure, enterprise database tables, or load scripts.
- 6. Perform data assurance checks of the NED and recommend Change Requests that will support the NED maintenance from GRC's authoritative source for directory information.
- 7. Provide assistance to the NASA Enterprise Applications Competency Center (NEACC) as requested.
- 8. Provide support for existing or future Agency-Wide Application Services (AWAS) as well as support to the NASA Data Center (NDC). Coordinate installation of AWAS software releases per NDC requirements and potential future AWAS applications.
- 9. Assist in the monitoring of the NASA Enterprise Applications Competency Center network activities to ensure GRC customers obtain maximum availability and support from the NDC.

10. Participate in NEACC-related meetings and conferences as requested by the NASA Enterprise Applications Competency Center and approved by TM.
11. Investigate reports for possible malicious incidents and pass on copies to the Office of the CIO Security Specialist.

## 36.00 Multimedia Services

### **Videoconference & Collaboration Facility Scheduling & Operations (SOW Reference 3.6)**

#### **Summary:**

The GRC Videoconference Facilities require support in the areas of Coordination, Operations and maintenance. These support positions will be responsible for maintaining the schedule and providing front-line support for users of the videoconference facilities. In addition, the Coordinator will provide monthly and quarterly reports tracking usage statistics and maintenance status of the Code V owned rooms. This work area covers the following areas:

Building 3 Room 7, Room 113  
Building 50 Room 108  
Building 54 Room 232  
Building 60 Room 027  
Building 86 Room 100, Room 315  
Building 142 Room 186-1, Room 249, Room 260C, Room 290  
Building 301 Room 214  
Building OAI Room 1E4

The intent is to achieve cost savings by unifying scheduling for these rooms, to leverage the skills of Glenn customers to aid in operations, and to find common work elements that optimize the skills of the current PACE workforce.

### **Videoconference & Collaboration Facility Scheduling & Operations (SOW Reference 3.6.1)**

#### **Description**

##### **Overall Objectives:**

Provide Deskside operations support for Building 3 Room 7; on-call operations support and best effort maintenance support for the other non-NICS maintained rooms. Serve as primary focal point for scheduling all inbound and outbound GRC videoconferences for all video conference rooms at the center. The Coordinator/Operator will be responsible for maintaining the schedule and providing on-call support for users of the video conference rooms. As primary support person, this position requires a flexible start schedule so that the Coordinator/Operator can be available based upon room usage.

##### **Specific Work Requirements:**

1. Simultaneous support of Bldg. 3 and back-up facilities
2. In the event that Bldg 3 is booked, provide fractional FTE tech support for startup and teardown of a ViTS back-up facility with on-call support during the conference (operator does not stay at back-up facility during conference).

3. Provide a common, efficient mechanism for customers to schedule a videoconference at any of the specified rooms that meet their needs.
4. Provide a location to customers one to two days in advance of their upcoming conference.
5. Coordinate the scheduling of conferences with the NISN Agency videoconference system managed out of MSFC. This includes accessing the NISN online scheduling system to reserve a time slot and bandwidth with the NISN operated bridge.
6. Maintain established gov't web-based calendar (e.g. Webevent) of conferences
7. Provide on-site staff at Building 3 Room 7 during each videoconference conducted at this location. Senior GRC executives frequently use this room and expect this level of service. This will be considered deskside support.
8. Perform conference setup at the ViTS back-up facilities in Building 142, Rooms 186-1, 230, and 290 as needed. This involves establishing (i.e. dialup) the conference prior to actual start time, insuring that all equipment is functioning properly, and taking action to repair or coordinate problems observed during startup. Disconnect conference after completion.
9. On an as available basis, provide staff to perform or coordinate troubleshooting and problem resolution during ViTS back-up facility conferences. This will be considered best effort support.
10. Support established agreements with occupants in Buildings 3/113, 50, 54, 60, 86, 301, 142/290, OAI and Plumbrook to arrange for onsite personnel to perform conference setup/disconnect and to be available for best effort support
11. Compile and submit monthly reports to the government showing the utilization of each room and the customers for all rooms. Compile and submit weekly highlights as needed to bring specific concerns or issues to the attention of the task monitor.
12. Gov't will assist the contractor in establishing bumping guidelines and priority users for each room.
13. Conduct periodic maintenance per agreed plan/schedule and provide a current/historical status of maintenance actions upon request.

### **Advanced Engineering Collaborative Room Support (SOW Reference 3.6.2)**

#### **Description**

##### **Overall Objectives:**

This work area provides support for the operational Advanced Engineering and Engineering collaborative rooms designated below. In particular, this effort will provide video, audio and other system support to maintain and operate the rooms in an efficient and effective manner. The support required includes the following: technical support for the use of facilities, the routine maintenance and diagnosis of the collaborative equipment and support of users and or activities in the collaborative rooms.

##### **Specific Work Requirements:**

Provide support for administrative duties of the computing/collaborative infrastructure and integration duties:

1. Support of collaborative environments (video, audio, and data sharing) as needed by the customer.
2. Integration of Engineering software and collaborative tools for use by Engineering Design teams (network access, platform interdependencies, etc).
3. Coordinate and schedule regular maintenance, new system integration, and equipment repair issues.

4. User support to utilize the collaborative rooms to their fullest potential.

**End Products:**

Maintenance and operational support of designated rooms.

## 37.00 – IT Risk Management and Security

**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. The OCIO 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 work area is to provide network security support to the Risk Management and Security Office in accomplishing its multifaceted mission including support to Privacy data management and oversight.

Currently, network security support personnel use a host of IT hardware and software to preserve the integrity of the network. Hardware includes: Sun Servers, Intel Workstations/Servers, Cisco routers and switches. Software includes: Sun Solaris, Linux, Windows, Sendmail, Apache Web Server, Network Intrusion Detection, Log Management, Data Loss Prevention, Firewalls, Web Content Filter, Secure Shell (SSH), Kerberos, and Secure Sockets Layer. Those supporting this work area currently maintain servers in the internal security services network as well as distributed across the enterprise for various security purposes.

### **IT Security Management and Operations (SOW Reference 3.7.2)**

**Overall Objectives:**

The PACE team will provide support for the vulnerability scanning of all hosts and web application on the GRC network. Reports will be submitted to the GRC CISO, designated customers, and agency in a timely manner as directed. Customer outreach and interaction is required to ensure success of mitigating vulnerabilities. Log aggregation services will be provided with high availability services and end-user support.

**Specific Work Requirements:**

1. Web Security
  - a) Provide system administration support of the Hailstorm web scanning application and WebDefend web monitoring appliance. This includes website access

management as well as role-based access management to these resources when applicable.

- b) Assist in investigations as required and under the direction of the GRC CISO.
- c) Conduct website vulnerability assessments bi-annually at a minimum.
- d) Assist website administrators in identifying corrective actions which mitigate findings from vulnerability assessments.
- e) Work with the Agency Web Application Scanning Program (WASP) to support and arrange scanning activities. Utilize findings of the scanning activity and work with application owners to mitigate web site and application security vulnerabilities.
- f) Participate in agency meetings as required.

## 2. Vulnerability Scanning

- a) Assist in investigations as required;
- b) Conduct monthly vulnerability scans to support the Agency vulnerability scanning requirement;
- c) Conduct quarterly credentialed vulnerability scans to support the Agency credentialed scanning requirement (quarterly credentialed scans will meet the monthly scanning requirement for the month the credentialed scans are conducted);
- d) Ad-hoc support to meet NASA customer requirements when requested;
- e) Participate in agency meetings as required.

## 3. Security Management and Operations (Central Log Management)

The PACE team shall provide support for various programs and projects for GRC as directed and prioritized from the Risk Management and Security Office in regard to administration of management of the SPLUNK GRC Glenn Log Intelligence Management System (GLIMS). This includes:

- a) Consult users in the benefits and use of GLIMS,
- b) Administer accounts,
- c) Develop an evolving data analysis process for GLIMS logs.
- d) Monitor critical logs continuously for abnormal activity and security threat. Review logs on a daily basis.

## 4. System Validation for Network Access

The Contractor shall research, validate, and approve requests which grant or modify access to the GRC network for individual computer systems. For each request that is received, the Contractor shall utilize available database tools and contact customers as necessary in order to make an initial determination whether the request for network access meets key system-level IT security criteria.

- a) Criteria that shall be factored into the determination:
  - i. The system access must be included in a valid NASA System Security Plan.
  - ii. The system has undergone a system vulnerability scan. Exception: The system has not been scanned because it needs to be on the network to be scanned and it is currently scheduled to be scanned.

- iii. The system has an up-to-date KACE patching agent installed. Exception: The running operating system does not support KACE.
  - iv. The system has undergone an assessment for personally identifiable information.
  - v. If the system is running and Mac or Microsoft Windows operating system, the system will become a member of the NDC Domain. Exception: A waiver is granted by the CISO.
- b) Acceptable outcomes for each request:
- i. Approve: The system has met the above criteria for network access.
  - ii. Deny: The system has not met the above criteria for network access.
  - iii. Pending: There is not enough information at a particular time to make a determination. If this is the outcome, then a reasonable effort to collect the required information shall be performed, and an alternative scheduled expectation to make a determination on the request shall be documented.
- c) The initial recommendation for each request shall be determined within 24 hours of receiving the request.

The Contractor shall document all supporting information gained from customers or research, and document all final recommendations for each request, including an itemized acceptance of the individual criteria.

**End Products:**

1. A highly reliable and proactive Security Management and Operations posture to GRC IT security threats.
2. A team which provides the foundation for success in plans, programs, and customer outreach activities of the IT Security Program Office;
3. Technical documentation and white papers completed as requested by the customer;
4. Documented verification of all information system configuration changes when made.

**IT Security Incident Response (SOW Reference 3.7.4)**

**Overall Objectives:**

The PACE Incident Response (IR) team will conduct investigations relating to malicious code and digital forensics of suspected IT Security incidents. This activity will be under the authority of the Center Chief Information Security Officer (CISO) or GRC Incident Response Manager (IRM). The team will interact with other investigative units and other agencies as required. In rare cases, representation by the incident responder may be required for court proceedings.

**Specific Work Requirements:**

1. Monitoring activities associated with IR in conjunction with the network team (NICS Contractor);
2. Provide immediate response and handling of IT security incidents in accordance with ITS-HBK-2810.09-02, Incident Response and Management: NASA Information

- Security Incident Management. Incident Response personnel conduct investigations, and submit findings under the direction of the Government.
3. Examination of hard drive disk data, up to and including analysis and review;
    - a) Includes RAIDs, servers, laptops, and desktops;
    - b) Follow best-in-class (legally accepted) digital forensic methodology;
    - c) Conduct review of network-based traffic for both malicious incidents, as well as digital forensics;
    - d) Examination of a multitude of file formats to include:
      - i. Email
      - ii. Documentum (MS Word/Rich Text Format/Open Office, Portable Document Format [PDF])
      - iii. Graphic files (Joint Photographic Experts Group [JPEG[JPG]], Tagged Image File Format [TIFF], Bit Map Picture [BMP]);
    - e) IR team members will review of multitude of log formats that include, and not limited to:
      - i. Splunk (GLIMS) data aggregator
      - ii. Data Loss Prevention (DLP)
      - iii. Server Log Data
    - f) Reporting of IR findings to appropriate parties that are involved with the case[s]. This information will be filtered to the Incident Response Lead (IRL) and IRM prior to dissemination with other parties.
      - i. Communication is based on a need-to-know.
      - ii. Approved parties include but are not limited to:
        1. Human Resources
        2. Criminal Investigations
        3. Legal
        4. Other parties to be involved with an incident will be determined by the IRL and IRM
    - g) In conjunction with IR duties, the IR team may be required to review network and firewall logs.
    - h) Disconnecting of suspected compromised equipment from the internal Glenn Research Center (GRC) network at the direction of the Chief Information Security Officer (CISO) or GRC IRL.
    - i) Disconnect active accounts at GRC under the direction of the CISO, IRL or IRM
    - j) Open communication with other security team members about emerging threats, and vulnerabilities
      - i. This is a Critical to Quality (CTQ) for the IR team and will be continually under development
    - k) Documenting IT Security investigations and providing testimony if required per NIST SP 800-61. IR Team Services/Responsibilities include the following items:
      - i. Advisory Distribution: New vulnerabilities awareness and incident information distribution to parties with a need to know.

- ii. Vulnerability Assessment: This aspect is handled by the Agency SOC unless otherwise requested by the customer. If requested, the incident handler is responsible for conducting the vulnerability assessment/analysis.
  - iii. Intrusion Detection: This is handled by the Perimeter Support team (NICS), however a responsibility exists to correlate data against suspected intrusions.
  - iv. Education and Awareness: Incident Handlers shall work with training staff as requested to ensure Industry/GRC/Agency best practices and policies are followed.
  - v. Technology Watch: Incident Handlers are responsible for tracking trends in information security threats including use of trends when available.
  - vi. Patch Management: This requirement refers to Incident Handlers having access to Patch Management data to assist in analysis of security investigations.
- l) Support Law Enforcement and Office of Inspector General.
  - m) Support Criminal Investigation Unit.
  - n) Support GRC Human Resources and Legal departments in investigations.
  - o) Review and completion of incidents and tasks assigned by the SOC.
    - i. Investigation and priorities given by the IRL and IRM will take precedence over normal daily security requests.

End Products:

1. A highly reliable and available Incident Response architecture which responds to IT security threats of the Center;
2. Technical documentation and white papers completed as requested by the customer;
3. Documented verification of all information system configuration changes when made;
4. Information sharing regarding emerging threats when appropriate or as directed.

**Program Protection (FISMA Compliance and Support) (SOW Reference 3.7.5)**

Overall Objectives:

Team PACE will provide support for the development, certification and accreditation of the GRC Common Security Control Baseline and consulting support to individual plans throughout the center as well as support FISMA compliance reporting requirements as directed by the Agency.

Specific Work Requirements:

Track and assist GRC organizations in IT security planning processes to include:

1. Work with Organizational Computer Security Officials (OCSOs) to improve the overall security knowledge and posture of NASA GRC through layered defense strategies applied to systems within the GRC perimeter;
2. Support for the development, certification and accreditation of the GRC Common Security Control Baseline and consult OCSOs, system owners and system administrators of individual plans throughout the Center to meet FISMA compliance and reporting in accordance with the Federal Information Security Management Act of 2002 (FISMA).

3. Support Certification and Accreditation throughout its lifecycle, particularly in the Continuous Monitoring phase.
4. Track and assist GRC Organizations in the Security Planning process. Develop and maintain Center Master IT Security Plans and associated subordinate plans.
5. Respond to data calls and review policies as requested by the customer;
6. Perform analysis of FISMA, NPR, NIST, or other applicable documents or standards.
7. Facilitate, and when appropriate, conduct technical and non-technical security control audits;
8. As resources permit:
  - i. Facilitate and/or conduct IT security risk assessments and Business Impact Assessments for GRC Organizations as they are requested.

**End Products:**

A team which provides the foundation for success in plans, programs, and customer outreach activities of the IT Security Program Office;

1. Technical documentation and white papers completed as requested by the customer;
2. A Center-wide Assessment and Authorization program with clear communications and end-user System Security Planning support.

**Information Protection (Privacy Management) (SOW Reference 3.7.6)**

**Overall Objectives:**

The PACE team will provide support in the area of Privacy Management as directed and prioritized by the Glenn Research Center (GRC) Center Information Security Office (CISO) and Center Privacy Manager (CPM). Support will include but is not limited to working with Information System Owners (ISOs) to review and aid in ensuring compliance with all privacy requirements needed. Under the direction of the CPM, the PACE team will assist in validating the proper disposition and/or sanitization process for files and records which contain privacy information.

**Specific Work Requirements:**

In addition to the Overall Objectives, the contractor shall:

1. Support the CPM in Initial Privacy Threat Assessments (IPTAs) and Privacy Impact Assessments (PIAs);
2. Perform data collection for data calls as required;
3. Track PII policies and regulations;
4. Maintaining internal GRC databases in relation to the privacy program;
5. Support the CPM in conducting in-house training and mock Breach Response Team (BRT) exercises.
6. The Contractor shall support the completion and publication of System of Records Notices (SORNs) as described in NPR 1382.1 for identified Privacy Act Systems of Records.

**End Products:**

1. Support the foundation for success in plans, programs, and customer outreach activities for the GRC Risk Management Office and Privacy;
2. Technical documentation and white papers completed as requested by the customer;
3. State of IT Security monthly updates for tracking Privacy compliance.

## **IT Security Awareness and Training Center (SOW Reference 3.7.7)**

### Overall Objectives:

The Agency Information Technology Security Awareness and Training Center provides the Agency with tools to enhance knowledge and awareness of different aspects of IT security through analogical methods. Work shall be performed in accordance with FISMA, NIST, OMB, ITS-HBK-2810.06-01 Awareness and Training, and ITS-HBK-2810.06-02 Awareness and Training: Role-Based Training Requirements.

### Specific Work Requirements:

1. Develop and implement Agency and GRC IT security awareness training as directed by the Government. This includes computer-based, classroom, virtual classroom, and individualized instruction.
2. Prepare and deliver briefings at the request of the Government
3. Maintain an understanding of learning and training concepts necessary for the development of IT security courses and the delivery of quality awareness products (e.g., newsletters, calendars, web sites) to support a wide range of topics related to IT security
4. Research and share the latest techniques, advances in courses, and awareness activities and serve as an administrator to the NASA learning management system (SATERN)
5. Assist the Government in staying in constant communication with the NASA Centers to determine needs as they relate to IT security awareness and training
6. Participate in outreach activities as requested by the Government
7. Assist with the collection, analysis, and accurate reporting of awareness and training metrics for the Agency and each NASA Center. Statistics shall be provided to determine the effectiveness of the activities and products delivered from the ITSATC.
8. Continuously track the completion of IT security training across the Agency and report to the Government.
9. Prepare and report metrics as requested by the Government
10. Provide assistance with FISMA reporting
11. Respond to data calls and review policies from the Agency, other Government organizations, and civilian authorities.
12. Participate in the coordination of the ITSATC and Agency Information Technology Security Division (ITSD) marketing programs
13. Support the development, review, modification, and implementation of IT Security training policies and governance.

### End Products:

1. Support the foundation for success in plans, programs, and customer outreach activities for the Agency Information Technology Security Awareness and Training program.
2. Technical documentation and white papers completed as requested by the customer;
3. State of IT Security updates for tracking Awareness and Training compliance and effectiveness.

## 37.01 – IT Risk Management and Security Code R

### **Summary:**

The Research & Technology Directorate (R&T, also known as Code R) at GRC is responsible for implementing IT Security Policy on a subset of its computer seats. These computers are those referred to as Network Attached Devices (NAD) and Maintenance (MA). When referring to the Code R computing environment, it is these specific computer types (NAD/MA) that are being addressed as the others are covered under a separate, vendor-managed security plan. The Code R directorate has already developed a set of comprehensive IT Security Plans describing an IT Security Policy for these seats. The intent of this work area is to provide Code R with an implementation strategy for this IT Security Policy and provide the plans and the resources to deploy that strategy into the Code R directorate production environment.

### **Overall Objectives:**

Team PACE shall provide functional and daily support in the area of network/host security as well as Code R IT Security Staff support as it relates to customer outreach and plans/programs for the Research and Technology Directorate.

### **Specific Work Requirements:**

Team PACE shall maintain a secured computing environment as approved by the Code R directorate Task Monitor. The Team shall perform the following duties during the execution of this work area:

### **Code R Security Engineering and Operations (SOW Reference 3.7.1)**

1. Develop the Code R IT Security implementation based on Code R IT Security policies.
2. Aid Code R IT Security Staff in devising optimum strategies for securing Code R IT resources so as to minimize cost/labor involved in its maintenance. Develop guidelines for the management/deployment of said strategies.
3. Manage the operation of the Code R IT Security Architecture implementation.
4. Work with Code R IT Security Staff to meet changing requirements. Propose, test, and implement enhancements for Code R IT Security Architecture design specifications and IT Security Policies, and recommend solutions and implement them upon approval of the Code R IT Security Staff
5. Identify equipment/software/services necessary for the Code R computing IT security infrastructure, and with appropriate government approval, obtain quotes from vendors, procure, deliver, evaluate and test necessary products to Code R.
6. Monitor network traffic and daily logs for abnormal activity and threat. The logs will be reviewed at least, but not limited to, every other day. Reports to Code R IT Security Staff will be provided when threats are noticed as well as the appropriate GRC and external

- parties. Provide data/logs or a secure interface to the information in response to requests from appropriate parties as determined by the Code R IT Security Staff.
7. Maintain awareness of latest security threats and respond to any threats to the Code R computing environment 24 hours a day, 7 days per week and take the appropriate actions to notify the designated government employee, as determined by Code R IT Security Staff, of threats and take the necessary steps to prevent further damage or intrusion.
  8. Provide technical documentation for existing and future Code R computing environment security system designs.
  9. Participate in the Glenn Research Center Computer Incident Response Capability. This includes the initiation of reports as discovered, the handling of incidents as appropriate, and attendance of meetings as defined by the team coordinator.
  10. Aid in the maintenance of Code R IT Security plans. Create, draft, and make changes to other Code R security related documents (policies, plans, assessments, etc.) as required.
  11. Provide IT Security guidance, guidelines etc. to Code R personnel. Work with Code R users to provide (when possible and appropriate) risk mitigating solutions that meet their requirements and maximize the security of the Code R computing environment.

#### **Program and Plans Support (SOW Reference 3.7.5)**

1. Provide support to Code R IT Security Staff to create, refine, and execute the procedures necessary to handle the security planning and revision process required by law.
2. Meet regularly with the Code R IT Security Staff to keep abreast of the latest issues that require attention and inform the Code R IT Security Staff on progress of the current work.
3. Create, draft, and make changes to security related documents (policies, plans, assessments, etc.) as required.
4. Support the writing and review process. Document creation, review, editing, publication, summaries will be provided as requested.
5. Create templates, announcements as requested.
6. Preparation of presentation material of significant vulnerabilities, risks, and practices which may counter them, as requested.
7. Assist in the identification of Code R NAD/MA systems by type and administrator such that vulnerabilities can be successfully traced to remediation and closure.
8. Track and assist Code R IT Security Staff in the Security Planning process.
9. Work with Code R IT Security Staff to improve overall IT security knowledge and posture of the Code R computing environment through layered defense strategies applied to Code R systems within the GRC Network Perimeter.
10. Meet regularly with assigned Code R IT Security personnel to create a relationship network where security issues can be communicated within Code R.
11. Facilitate IT security risk assessments for Code R Organizations, as requested.

12. Assist Code R organizations in the creation and preparation of IT Security Plans, Contingency Plans, and Risk Assessment Reports, as requested.

## 39.00 – Customer Experience

### **Summary:**

PACE Personnel will provide support to the Glenn I3P team as requested.

### **User Assistance Team (SOW Reference 3.9.1)**

#### **Overall Objectives:**

The Contractor shall establish and sustain operations of a local User Assistance Team (UAT) based on industry practices established by the Service and Support Professional Association. The Contractor shall provide users access to information about and assistance with OCIO products and services. UAT personnel shall stay apprised of the information that is provided through a recognized Help Desk/Technical Support Professional association and pursue ongoing professionally recognized customer support training and certification. The Contractor shall ensure as part of UAT operations, procedures and practices are in place to coordinate efforts with other service providers. The Contractor shall ensure as seamless an approach as possible to providing accurate, timely, and professional responses to customer request. The Contractor shall ensure a timely response and determine the most effective mechanism for future responses to similar requests.

#### **Specific Work Requirements:**

Incidents will be processed by the Enterprise Service Desk (ESD) through the NASA Shared Services Center Remedy system. ESD will then transfer appropriate ticket/Incident to the UAT. After receiving a ticket from ESD, the UAT will then transfer tickets/Incidents to the appropriate NON-I3P support groups.

1. The Contractor shall serve as an entry point for specific OCIO issues and services. Incidents will be processed by the Enterprise Service Desk (ESD) through the NASA Shared Services Center Remedy system. ESD will then transfer appropriate ticket/incident to the UAT. After receiving a ticket from ESD, the UAT shall then transfer tickets/incidents to the appropriate non-I3P support groups, including but not limited to eRoom, SharePoint, Application development requests, and Data Center services.
2. The support groups will also need access to the Government-provided ESD Remedy system. The ESD Remedy system will be used to assign, track, triage, and close tickets/incidents.
3. The UAT shall provide assistance to users with creating, submitting, modifying, and approving service requests and catalog requests.
4. UAT shall have the ability to transfer tickets/Incidents back to ESD through Remedy for appropriate resolution by Tier 2 contractors.

5. Answer all calls into the UAT Support Line, during 6:00AM – 6:00PM weekdays, ensuring where possible that the caller does not have to leave a voicemail. The Contractor shall implement a call logging capability. The Contractor shall respond to voicemail within two business hours and to e-mail within four business hours.
6. The UAT shall provide general support assistance to Glenn ESD Subject Matter Expert (SME) in the area of incident tracking, investigation, and workflow refinement and other I3P service and support duties as assigned.
7. Assist customers with ACES and NICS relate matters such as; ordering and tracking equipment orders, provide information and assistance to customer on “how to” questions (e.g. how to receive extended privileges).
8. Provide customer assistance on IT related special projects (e.g. student summer hire program).
9. Provide customer assistance on general IT related questions (e.g. printing problems, VPN access, move requests, ESD questions).
10. Work with other GRC contracts that have centralized point of contact functions directly related to their specific contract deliverables.
11. Sort, log, or respond to email received in the Customer Support mailbox. Email messages requiring a response shall be answered within four business hours.
12. Provide accurate tracking, routing and reporting of the customer requests.
13. Ensure that all customer requests, where appropriate, are routed to the appropriate solution provider, logged, tracked and completed in a help desk tool. This includes logging of requests and a focus on ensuring that solutions are recorded as part of the closure process of open items. The Contractor shall ensure that processes facilitate easy analysis of the current workload (frequency and type of service). The Contractor shall ensure that information processed can be used as a knowledge base designed to capture workload metrics as well as information that is useful to Government personnel, management, and the GRC community at large (e.g., knowledge base of standard processes, issue patterns, lessons learned to future support).
14. The Contractor shall support the development and submission of Knowledge Articles, and their integration with the Enterprise Service Desk (ESD), at the direction of the GRC ESD SME.
15. Provide assistance to users for the submission and processing of service requests. This support includes working with the OCIO organizational liaisons on submitting requests, tracking, providing status reports to the Government and customer. When contacted by the user, the Contractor shall provide support to users who experience rejected SRs, and assist users in correcting SRs in a timely manner.
16. Support product testing and user education on OCIO-provided products and services. The Contractor shall participate in various testing scenarios and in special teams to assess the capability or impacts of new or changing products and services.
17. The Contractor shall maintain a record of feedback and comments from customers.
18. Analyze data and produce reports as required. The UAT will provide weekly statistical and graphical reports of the number of incident responses, service requests and general assistance responses and collate the report data into weekly, monthly, quarterly, and other reports as required by the Glenn ESD SME.
19. Provide the following I3P related specific support:
  - a) Serve as the 1st level escalation of inquiries and issues that come to the User Assistance Team from the ESD, customers, or internal OCIO teams
  - b) Address problems/issues that are complex, unique, and/or involve multiple I3P service areas or services outside of I3P
  - c) Perform research as needed to assist the ACES SME in answering technical questions related to ACES services and delivery of those services to customers

- d) Provide assistance as needed in responding to actions from GRC Center and OCIO management and Agency I3P Service Offices
- e) Provide administration of the I3P SharePoint site
- f) Provide support as needed to the ACES and ESD SME's for the Agency and GRC CMDB efforts

End Products:

1. A highly reliable and available User Assistance Team which responds to user support requests at the Center;
2. Documentation and reports completed as requested by the customer;
3. Customer focused service;
4. Information sharing when appropriate or as directed.