Space and Naval Warfare Systems Center Atlantic
Technology Exchange

Kathryn Murphy
Senior Science Technology Manager (SSTM) for Software Engineering, 54000

28 November 2018
Welcome!

▼ Logistics:
- Refreshments
- Facilities
- Breakout sessions

▼ Survey Says!!

Agenda

Space and Naval Warfare Systems Center Atlantic Technology Exchange

Cloud Computing for Enterprise Resource Systems

28 November 2018

Hosted by:
Space and Naval Warfare Systems Center Atlantic

Location:
Space and Naval Warfare Systems Center Atlantic
New Orleans Office
2251 Lakeshore Drive
Building 3
New Orleans, LA 70122

0730 Arrival/Check-in/Networking
0815 Opening Remarks - Kathryn Murphy
0830 Panel Discussion on Cloud Computing for Enterprise Resource Systems – Moderator - Bradley Punch
0930 Networking Break
1000 Information Warfare Research Project (IWRP) Other Transaction Consortium – Don Sallee
1100 Break/Lunch
1200 Break-out Sessions
1630 Event Concludes
We deliver Information Warfare capabilities, including communication systems (radios), networking systems (routers/switches), cyber operations (red team/forensics/network defense), intelligence, surveillance, reconnaissance (sensors/decision support applications), business systems (benefits/personnel) and information security.
SSC Atlantic is part of the Naval Research & Development Establishment

- Comprised of scientists, engineers, mathematicians and supporting technical personnel who conduct DON research, development, test and evaluation.

- Encompasses the technical resources required to explore, develop and field future naval warfighting capabilities, such as laboratories, test facilities and test ranges.
SSC Atlantic
01E/40/50/70 Technical Leadership

Mr. Andrew Mansfield  Mr. Brad Hoisington  Mr. Peter Reddy  Dr. Suzanne Huerth

Statement A: Approved for public release; distribution is unlimited
Competency Aligned Organization (CAO)

Integrated Product Team competencies and departments cooperatively functioning together to produce goods and services.

Departments (cost, schedule, & performance):

- Fleet C4I and Readiness
- Expeditionary Warfare
- Enterprise Systems
- Shore C2ISR and Integration

Competencies (people, processes & tools):

1.0 Finance
2.0 Contracts
3.0 Office of Counsel
4.0 Logistics & Life Cycle Engineering
5.0 Engineering
6.0 Program & Project Mgmt
7.0 Science & Technology (includes Work)
8.0 Corporate Operations

Purpose

- Increase collaboration and communication between government and industry

Your Role

- Listen
- Contribute
- Learn

Ground Rules

- There are no procurements in play
- We are not contracting officers and cannot commit the government
- Just networking
Background
Contracts Industry Council

AFCEA Reps
▼ Patrick Burnette
▪ burnettegp@gmail.com
▼ Manny Lovgren
▪ mlovgren@lce.com
▼ Amy Bare
▪ amy.bare@baesystems.com

CDCA Reps
▼ Gary Jaffe
▪ gjaffe@atlas-tech.com
▼ Derrick Nixon
▪ derrick.nixon@kbrwyle.com
▼ Heather Walker
▪ walker.heather@bah.com

TASC Rep
▼ Paul Heim – WR Systems
▪ pheim@wrsystems.com

Statement A: Approved for public release; distribution is unlimited
Background
FY16 NDAA

SECTION 887. EFFECTIVE COMMUNICATION BETWEEN GOVERNMENT AND INDUSTRY

- “Not later than 180 days after the date of the enactment of this Act, the Federal Acquisition Regulatory Council shall prescribe a regulation making clear that agency acquisition personnel are permitted and encouraged to engage in responsible and constructive exchanges with industry, so long as those exchanges are consistent with existing law and regulation and do not promote an unfair competitive advantage to particular firms.”

DEPSECDEF MEMO dtd 2 MAR 2018

- “Our National Defense Strategy (NDS) directs our INTENTIONAL engagement with Industry to harness and protect the National Security Innovation Base as well as modernize key capabilities. Cultivating a competitive mindset requires we OPTIMIZE OUR RELATIONSHIPS WITH INDUSTRY to drive higher performance while always remaining within the letter and spirit of ethics and procurement regulations.”

Statement A: Approved for public release; distribution is unlimited
Technology Growth Areas
Investing in capabilities to outpace the threat of our adversaries

**Cyber Warfare:** Ensures availability, integrity, authentication, confidentiality and nonrepudiation of data sources.

**Data Science/Analytics:** Enables access and management of large quantities of data in structured and unstructured forms.

**Assured Communications:** Addresses the increasing demand for voice, multimedia and data transmission through wired and wireless communications systems.

**Cloud Computing/Big Data:** IT modernization and digital transformation for resilient infrastructure, platform and software services.

**Enterprise Resource Tools:** Supporting tasking across the software life cycle, to include operational support for major commercial ERP systems or a custom solution for business/logistics decision systems across the Navy Tactical Command Support System.

**Collaboration/Social Networks:** Allow social interaction to be aggregated, assessed and pushed back into the supporting systems as structured data that can be used for better decision-making.

**Autonomy:** Enabling systems to adapt their actions to changes in their mission and operating environment without the intervention of a human operator.

**Embedded Systems:** Operation of computer systems that perform a particular function within a larger system without direct human interactions.

**Mobility Solutions:** Provide wireless technology and infrastructure authentication and connection to the enterprise providing the warfighter the ability to engage with a mobile environment anytime, anyplace.

**Model-Based Systems Engineering:** Technologies used to support the development, management, and application of virtual constructs of varying fidelity across the spectrum of systems engineering.

**On-Demand Manufacturing processes:** Produce products and/or components, when or as they are required at the point of use, using additive and/or traditional manufacturing methods.

---

**Statement A:** Approved for Public Release. Distribution is unlimited (19 June 2018).
Technology Exchange Overview

Technology Growth Areas

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Science &amp; Analytics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Warfare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assured Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autonomy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Computing for Enterprise Resource Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-Demand Manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model-Based Systems Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tech Ex Attendance

Tech Ex Survey Data
Survey Comments

“I thought that the Technology Exchange Forum was informative and beneficial for industry. It gave a better understanding of where SPAWAR is looking to go with cloud computing and data science technologies. I do think it would have been helpful for industry to be involved with the panels before we submitted whitepapers. It would give us the opportunity to better tailor our offering”.

“The networking alone was worth the drive, the panel was just the icing on the cake.”

“Some of the speakers were hard to understand (mics were too far away).”

“Information discussed during the technical panel was useful. I also appreciated the opportunity for a one-on-one exchange with the technical team. This has been long overdue!”
Save the Date!

Next Technology Exchange: March 2019

Location: TBD

TGA Focus Areas: MBSE and TBD
Cloud Computing for Enterprise Resourcing Panel

Moderated by:

Bradley Punch
PEO EIS Deputy Technical Director
## Panel Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew Tash</td>
<td>PEO EIS: Technical Director</td>
</tr>
<tr>
<td>Charmaine Narciso-Jiao</td>
<td>PEO EIS: Deputy APEO-Engineering</td>
</tr>
<tr>
<td>Thai Ly</td>
<td>PMW 270 Navy Commercial Cloud Service (NCCS) Project Office: Project Support</td>
</tr>
<tr>
<td>David Spencer</td>
<td>PMW 250: Technical Director Team – Cloud Lead</td>
</tr>
<tr>
<td>Robert Neuman</td>
<td>SSC Atlantic: Cloud Tech Services IPT Cybersecurity</td>
</tr>
</tbody>
</table>
Design In & Sustain Cybersecurity, Reliability, Agility, Affordability*

Build Intent-Based Leadership, and Business and Technical Acumen into our Workforce Culture*

*ASN/SECNAV Pillar Alignment
PEO EIS Strategy

MISSION
We deliver modern, secure, and effective enterprise information technology systems and services

VISION
To provide the premier enterprise information technology and business system user experience

STRATEGY

Enhance data-driven decision making
- Shift to the Cloud
- Make mobile "the way we work"
- Deliver modernized applications and services
- Enhance enterprise network performance
- Leverage data analytics

Deliver an enhanced and positive customer experience
- Improve customer satisfaction
- Implement and improve user-centric design principles
- Improve service fulfillment response time
- Enhance self-service capabilities

Increase agility and drive affordability
- Eliminate gaps between industry and government
- Modernize processes associated with acquisition
- Adopt a services first IT acquisition strategy
- Modernize enterprise networking and business systems
- Maximize automation in systems and services

Develop and maintain a workforce driven by modern IT and continuous process improvement
- Improve workforce satisfaction
- Empower the workforce
- Train the workforce
- Increase workforce recognition

Improve workforce satisfaction
- Empower the workforce
- Train the workforce
- Increase workforce recognition
Technical Exchange Topics

1. Enterprise Cloud Transformation
2. Digital Core Services
3. Digital Transformation
4. Modern Service Delivery

Industry ideas desired to improve cloud adoption and achieve digital transformation
Objective State - 2021

Operational View
Aligned with DoD Cloud Computing Strategy Overview

Our plan is to migrate 100% to cloud computing through a combination of on-prem and off-prem clouds with a common platform for interoperability. Delivering capabilities via cloud is critical to meeting Navy mission at speed and driving affordability.

Digital Core Services enables enterprise-wide management, security, operations, and analytics for agile decision making; supports interoperability, portability and development.

Navy Cloud First Policy signed in Feb 2017 requires use of Commercial Clouds and reduction in legacy on-premises data centers.
Cloud Adoption Model

Level 1: Awareness + Preparation (2011-2013)
- Initial Customer Cloud Training
- Data Center Consolidation prepared systems for virtualization and enterprise services

- Initial contracts
- Initial production deployments
- Pilots - DEVSECOOPS (C2C24), CSCCA, SaaS, Public Cloud

Level 3: Proactive + Foundation (2018)
- Establish NCCS
- Cloud-first Policy
- Broker Delegation
- Enterprise Contract
- Standard C2 Language

Level 4: Service Aligned + Exploitation (2019-2021)
- Standards Development
- Mature cybersecurity process
- Automation & Templates
- Task Orders on Enterprise Contract
- Fuse Portfolio Management, Data, Cloud and Operations Governance

Level 5: Business Partner + Hyper Cloud (2022+)
- Accelerated adoption finishes here
- Cloud Native Apps
- SaaS Ecosystem
- Common Operational Backplane
- Digital Core Services

Navy is here
Current State - Silos

- Legacy & Redundant Applications
- Siloed Digital Core Services
- Siloed Infrastructure

**FAMs**
- MPT&E
- LOG
- ACQ
- CIVPERS
- FM
- C2
- INTEL
- RDT&E
- LEGAL

**Duplicated Work**
**Integration Challenges**
**Distraction from Core Missions**

**LACK OF ENTERPRISE OVERSIGHT**
Future State - Digital Core Services

- Simplified User Interface
  - Functional End Users
- Enterprise-Wide Digital Core Services
  - Ex. IdAM, Authoritative Data Environment
- COMMON INFRASTRUCTURE
  - Ex. Fleet Cyber (Enterprise owner of security)
- Transport
Secure access to services and data anytime, anywhere and from any device (ubiquitous access)

1. **DEVICES**
   Services and data are equally accessible across all devices (device agnostic).

2. **ACCESS**
   Multiple connectivity methods for managed and unmanaged devices.

3. **IDENTITY**
   Device, access and user combinations are verified.

4. **APPLICATIONS**
   User centric services designed for ubiquitous access.

5. **DATA**
   Seamless data synchronization across all devices.

6. **PROCESS/GOVERNANCE**
   Mobility is not a separate technology, it is the expected outcome of all our IT and governance working together properly to reduce parity between on-network and off-network capabilities.
PEO EIS APEO-E
Charmaine Narciso-Jiao
CHENG’s Top Priorities

▼ Cybersecurity
  ▪ Integrate cybersecurity and interoperability upfront through System of Systems Engineering to design for Fleet Cyber Resiliency

▼ End-to-End Technical Authority and Certification Authority
  ▪ Ensure that products delivered to the Fleet are technically sound and self-sustaining

▼ Going Digital
  ▪ Drive alignment, collaboration, integration and efficiency to operate as a coherent Navy enterprise – F A S T!

Mission Engineering @ Lightspeed
SPAWAR’s Model Based Systems Engineering Policy

Key to “Going Digital” is a framework that will provide a “single source of truth” through the formalized use of a common model to support a data driven systems engineering lifecycle that can be used to support acquisition and budgetary decisions while ensuring interoperable designs and capabilities throughout the SPAWAR Enterprise.

Objectives:
- Establishes Governance across major SYSCOMS
- Provide consistent approach for developing and sharing engineering information across interrelated efforts
- Improves product quality, reduces cycle times, enables reuse and resource efficiency once implemented
- Enables Digital Thread

Technical Approach:
- Common Tools
- Common Repository
- Common Requirements Schema connected to model
- Common Data Dictionary
- Standard model templates/profiles
Objectives:
- Information Assurance
- Systems Management
- Core Enterprise Services
- Computing Infrastructure & Communications

Technical Approach:
- Identification Authentication and Access
- Configuration Protected Objects
- Boundary Protection Configuration
- Encryption Service, Forensics, Malware Protection
- Service and Application Discovery, IA Compliance
- Email/Calendar, File Transfer, SQL Database
- Office Productivity, Mobility, Knowledge Management
- DNS, LDAP
- Printers, Video, Workstations, VOIP, Servers, Wireless
- Cross Domain Solution Access and Transfers

Across multiple networks, there are common services that are currently provided by multiple product solutions. These products must separately be tested and certified for cyber resiliency as well as interoperability and sustainability not only within Navy but also with the DODIN. Providing common platform services will not only provide better buying power initiatives, it will also support improved cyber posture through common and inheritable solutions.
Integrated Platform as a Service (iPaas)

Multiple systems providing capability that is commercially available as one product. Examples include Human Capital Management, Payroll Systems, Talent Management Software, Customer Relationship Management.

Objectives:
- Use commercially available products
- Deliver capability incrementally and often

Technical Approach:
- Public Cloud
- Rapid Integration
- Agile Approach
- Configuration over Customization
- Leverage Application Program Interface Software products

Government Retains 100% Data Rights
Application Platform as a Service is a cloud service that offers development and deployment environments for application services. aPaaS platforms provide the ability to build applications iteratively, provision application software instantly, scale applications on-demand and integrate applications with other services.

Objectives:
- Build applications easily
- Deploy apps in minutes versus longer
- Scalability of the application
- Integrate with various other applications

Technical Approach:
- Visual Development
- Easy Integration connecting to databases, APIs, webservices and siloed data in legacy systems
- Multi device support
- Granular security to integrate with authentication providers
Data Strategy

Disparate data is reposed across multiple environments and is a challenge to integrate. Establishment of a common data strategy across the enterprise can allow data to be processed to deliver a capability without copying the data across multiple environments, which introduces risk to the data’s configuration and security.

Objectives:
- Federated Knowledgebase
- National to Tactical Integration
- Share Data Within and Between Platforms
- Timely Access to Enriched Data
- Consistent, Authoritative Data
- D-DIL Tolerant
- Expose All Data for Analytics
- Facilitate Cybersecurity

Technical Approach:
- High Side Fusion
- Security Labels and Tags
- Identity and Access Management (IDAM)
- Cross Domain Solutions
- Gateway Services
PMW 270 (NCCS)
Thai Ly
PMW 270 Mission

- **Mission**: Under the Navy’s Commercial Cloud Brokerage model, Program Executive Office for Enterprise Information Systems (PEO EIS) is the designated Navy Enterprise Cloud Brokerage Executive Agent (EA) responsible for developing and executing the overarching cloud brokerage structure, with the purpose of supporting accelerated Navy adoption of commercial cloud technologies and services while protecting all Navy information in the commercial cloud. These functions are executed by PMW 270, the Navy Commercial Cloud Services (NCCS) Project Office.

- **Direction**: DDCIO(N) Memo of 1 Feb 17, NAVY CLOUD FIRST POLICY, DDCIO(N) Memo of 19 Dec 17, NAVY COMMERCIAL CLOUD BROKERAGE POLICY

- **Objectives**:
  - **Navy Cloud Brokerage (NCB)**: Promulgate NCB policy and governance; Support NCB stand-up and commercial service development; Develop, collect, and assess NCB metrics.
  - **Navy Cloud Outreach and Readiness**: Develop Navy Cloud engagement plan; Provide web and classroom-based Cloud training opportunities; Enable access to Cloud readiness and portfolio prioritization resources.
  - **Navy Cloud Acceleration**: Launch and maintain Navy Cloud resource portal; Award Navy Commercial Cloud contract vehicle; Enable access to cloud modernization and migration resources
Challenges

- **Time and uncertainty between concept and operation**
  
  **Problem statement:** Systems today are building/rebuilding systems as they migrate to new environments, datacenters and cloud. Takes about 20-40 days to build, install and secure a system.
  
  - Time between CSP Service GA to FedRAMP to DoD PA is long
  - Not leveraging cloud native solutions that are already PAed
  - Length of time to complete RMF process
  
- **Where industry can help:**
  
  - Templates and Repeatable processes: Baseline builds/Images, build out/lockdown scripts,
  - Infrastructure as Code: Blueprinting, Configuration drift, Monitoring,
  - PaaS / SaaS solutions

SCALABLE, RESILIENT, SECURE CLOUD
Challenges

• Cybersecurity at Scale

  – **Problem statement:** Current solution providers are not able to respond to changing cyber requirements (e.g. WAF, RWP, PCAP) at scale
    • Multiple teams / organization support – NCDOC, NAO, CAP provider, VDSS Provider, VDMS Provider, Mission Owner

  – **Where industry can help:**
    • Be able to buy SCCA (CAP, VDSS, and VDMS) as a service to reduce procurement cost and implementation timeframe
    • Be able to scale with demand and be flexible to adjust to Cyber requirement changes
    • Take advantage of cloud services beyond compute, storage and networking

SCALABLE, RESILIENT, SECURE CLOUD
PMW 250
David Spencer
Problem Statement:
Many distributed applications with disparate architectures and no common metrics or methods to monitor health. [Use Case: DON TRACKER]

Objectives:
- Best of breed application monitoring capability offered as a DISA provisionally authorized service to application owners through standard interfaces

Technical Approach:
- Agnostic
Problem Statement:
Difficult to mimic the operational environment during development and developmental test [Use Case: All portfolio]

Objectives:
- Best of breed load testing capability offered as a service to application developers and testers.
- Can spin up and down on demand.
- Supports DoD/DoN identity management standards.

Technical Approach:
- Agnostic
Problem Statement:
Find threshold for commonality in application development/deployment across portfolio of disparate application types and architectures and provide common Continuous Integration Continuous Development (CICD) toolset and/or services to support [Use Case: All portfolio]

Objectives:
- Common CICD services in use by multiple application development teams.
- Provided as a service to application developers as GFE/GFI/GFP

Technical Approach:
- Agnostic
Problem Statement:
Keeping pace with digital transformation and the impact on user experience for customer engagement; using data to improve user experience [Use Case: Navy 311, NESD]

Objectives:
- Customer support strategy/tools which leverage modern communication channels. Data collection, analytics, and machine learning to improve communications.

Technical Approach:
- Agnostic
Problem Statement:
Difficult to find content management solutions that are accessible, intuitive, and reliable while meeting the DoD/DoN authentication standards without incurring significant technical debt [Use Case: iNAVY, DON Tracker]

Objectives:
- Best of breed content management capabilities offered in a SaaS model which are effectively governed and support DoD/DoN identity management standards and digital loss prevention.

Technical Approach:
- SaaS offering
- Must support PKI (CAC)
Problem Statement:
The Navy has not been able to take advantage of many recent, innovative Identity and Access Management (IdAM) solutions offering secure authentication by alternate means, intelligent policy/permissions management, and authorization flexibility. [Use Case: All portfolio]

<table>
<thead>
<tr>
<th>Objectives:</th>
<th>Technical Approach:</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Best of breed IdAM solution, accredited (ideally for IL-4 workloads), and offered as a service</td>
<td>▪ Agnostic</td>
</tr>
<tr>
<td>▪ End-to-end solution, covering:</td>
<td></td>
</tr>
<tr>
<td>▪ Access Management (AuthN/AuthZ, CAC-PKI, BYOD MFA, SSO, Federated ID mgmt.)</td>
<td></td>
</tr>
<tr>
<td>▪ Identity Management (Self-service remediation, delegated administration, automated approvals, enterprise role definition)</td>
<td></td>
</tr>
<tr>
<td>▪ Holistic directory services (aggregating existing AD/LDAP/etc., transforming to updated directory services with normalized attribute stores)</td>
<td></td>
</tr>
<tr>
<td>▪ Auditing and Compliance (logging, monitoring, access certification, and reporting)</td>
<td></td>
</tr>
</tbody>
</table>
SSC Atlantic Cloud Tech Services IPT Lead
Robert Neuman
Problem Statement:
Enterprise Cloud migration is broader than a single application, it is predicated by business planning and portfolio discovery; executed using Migration factories and/or teams that apply Rehost, Refactor, Revise, Rebuild and Replace methods at the application level using automation for provisioning and testing; and operated using enterprise scale tools to provide application performance management software with active use of automation components.

Objectives:
- Migration strategies, training, and tools that enable migration to and operations within the cloud at scale across multiple providers and networks including afloat.
- See DON Combined Application Hosting Standard

Technical Approach:
- Within bounds of DOD and DON Security and contracting requirements.
- Needed deviations or waivers of DOD and DON Security and contracting requirements identified and substantiated in proposal.
Problem Statement:
Enterprise migration and rationalization of applications necessitates the automated transfer of data based on rules with activities for data remediation to improve the quality of data, eliminate redundant or obsolete information, and match requirements of new systems. Methods include creating centralized or decentralized within the team’s, Center of Excellence and developing the deep business knowledge needed by the teams.

Objectives:
- Migration methodologies, training, and tools that enable data migration to and operations within the cloud at scale across multiple providers and networks including afloat.

Technical Approach:
- Within bounds of DOD and DON Security and contracting requirements.
- Needed deviations or waivers of DOD and DON Security and contracting requirements identified and substantiated in proposal.
Problem Statement:
Accurate knowledge of systems is necessary to perform migration assessments needed for decision making and to maintain a secure and performant environment. Instant and accurate inventories are necessary for cyberdefense.

Objectives:
- Detailed Capabilities to inventory and survey on premise application landscapes for the required data to select a migration path and enterprise tools to provide application performance and security management. See Software Application Distribution Standard

Technical Approach:
- Within bounds of DOD and DON Security and contracting requirements.
- Needed deviations or waivers of DOD and DON Security and contracting requirements identified and substantiated in proposal
Problem Statement:
Enterprise level decisions need accurate information regarding lifecycle costs past and future to facilitate budget inputs and plan accurately. Due to the fixed budget methods are needed to facilitate cost control activities.

Objectives:
- Cost monitoring methodologies, policies, processes, and tools that enable the monitoring and prediction of application lifecycle costs. Corresponding methodologies, policies, processes, and tools to automate operations within a budget window. See Combined Application Hosting Standard

Technical Approach:
- Within bounds of DOD and DON Security and contracting requirements.
- Needed deviations or waivers of DOD and DON Security and contracting requirements identified and substantiated in proposal.
Objectives:
- Recommendations for long-term strategic initiatives across departments and organizations that focus on all aspects of IdAM, and not just the technology to be deployed. This includes the development of trust models across departments, organizations, and external entities, ensuring assurance levels are uniform for authentication purposes, and defining security policies around authorization and access management. Examples include: Multi persona, distributed, and alternate token capabilities, Attribute monitoring and awareness (training status, leave, etc.) see Identity and Access Management (IdAM) Standard

Problem Statement:
IdAM cuts across numerous programs, and systems within the Navy and DoD enterprise, which are typically directed and managed separately. Behind the technology and the solutions that are deployed is the governance and policies needed for solutions to be successful from a mission, business and security perspective.

Technical Approach:
- Within bounds of DOD and DON Security and contracting requirements.
- Needed deviations or waivers of DOD and DON Security and contracting requirements identified and substantiated in proposal.
Any Remaining Questions/Comments?
SPACE AND NAVAL WARFARE COMMAND

Information Warfare Research Project

Technical Exchange New Orleans, LA
28 November 2018

Mr. Don Sallee
SSC Atlantic
IWRP Program Manager

SPAWAR is part of the Naval Research & Development Establishment (NR&DE)
What is the Information Warfare Research Project (IWRP)?

- SPAWAR established the IWRP to meet the need to rapidly advance IW technologies to the warfighter.
- The program’s efforts focus on the research and development of the underlying technologies that advance naval IW capabilities.

IWRP uses Other Transaction Authority (OTA) to:

- Greatly increase speed to award
- Reduce barriers to competition
- Increase access to innovative commercial solutions
- Leverage advanced commercial technologies

OTA provides the ability for rapid:

- Innovation
- Prototyping
- Fleet fielding

Advancement of IW Technologies to the Warfighter
What is IWRP Consortium?
How does it work?

Commercial Businesses
Manufacturing
Academia

Nontraditional Partnering

Traditional Industry Partner (normal DON business)

Traditional Partnering

IWRP Consortium

Teaming
Innovation
Prototyping
Collaboration

Advancing Naval Information Warfare Through Rapid Prototyping on a Global Scale
Industry Initiated Ideas (I³) Process Overview

1. Technical research idea identified
   - Workforce Capability Gaps
   - Technical Growth Areas
   - Laboratory Improvements
   - NRDE Goals

2. Appropriation Type Identified
   - RDT&E
   - OPN
   - O&M

3. $ Budget Set
   - Gov't Technical SME's Identified

4. Enhanced whitepapers

5. SMEs make Selections for Oral Presentation

6. Project Oral Presentations to Gov SME

7. Project Selection And RFP

8. Proposal Evaluation and Award

9. Project Execution and Closeout

Industry Initiated Ideas (I3)
Project Follow-up

10. Technical Gov’t SME Oversees PPA Execution

11. Technical Gov’t SME or Consortium Member
Brief technical information at event for workforce development

12. Project Artifacts Saved in Repository

Getting the Most from All Projects

What is a Prototype?

Used to evaluate the technical or manufacturing feasibility or military utility of a particular technology, process, concept, end item, effect or other discrete feature.

Can be:
- Proof of concept
- Pilot
- Novel application of commercial technology for defense purposes

May include:
- Systems
- Subsystems
- Components
- Materials
- Methodology
- Technology
- Processes
- Agile development activity

Creation, design, development, demonstration of technical, evaluation or operational utility
Or a combination of the above
IWRP Technology Areas

- Cyber Warfare
- Data Science/Analytics Technologies
- Assured Communications
- Cloud Computing
- Enterprise Resource Tools
- Collaboration and Social Networking
- Autonomy
- Internet of Things (IoT) Embedded Systems
- Mobility
- Model-Based Systems Engineering (MBSE)
- On-Demand Manufacturing
- Technologies that would enable and improve Assured Command and Control (AC2)
- Technologies that would enable or improve Battlespace Awareness (BA)
- Technologies that would enable or improve Integrated Fires (IF)
IWRP Consortium Stats

Consortium Composition

Members

- Traditional: 178
- Nontraditional: 135

Members by Technology Area

- Battlespace Awareness: 87
- Integrated Fires: 39
- Assured Command and Control: 82
- On-Demand Manufacturing: 18
- Model Based Systems Engineering: 84
- Mobility: 60
- Internet of Things: 85
- Autonomy: 59
- Collaboration and Networking: 51
- Enterprise Resource Tools: 75
- Cloud Computing: 78
- Assured Communications: 109
- Data Science / Analytics Technologies: 136
- Cyber Warfare: 139

Production

Prototype Project Requests

- Total: 18
- Awarded: 0
- Pending Award: 0
- Responses Received: 54
- Sent To CMF: 10
- Routing: 2
- Forecast: 6
- Closed: 2

Workflow by Customer

- Closed
- Other
- Forecast
- PAC
- LANT

FY19 Projected Schedule

www.theiwrp.org

Start Execution

LANT Qtrly Mtg Charleston, SC

PAC Qtrly Mtg San Diego, CA

LANT Qtrly Mtg Stafford, VA

PAC Qtrly Mtg San Diego, CA

Project Panel ASSY

Allow CLASS PPAs

4 December CDCA Annual Mtg

Decision Point Increment 2

We are here

FY19

Points of Contact

**SSC Atlantic**
- **Don Sallee** – Program Manager
  - donald.sallee@navy.mil
- **Lisa Rosenbaum** – Agreement Officer
  - lisa.rosenbaum@navy.mil

**SSC Pacific**
- **Vince Squitieri** – IWRP IPT Lead
  - vincent.squitieri@navy.mil
- **Sharon Pritchard** – Agreement Officer
  - sharon.pritchard@navy.mil

To become a member of the IWRP consortium go to https://www.theiwrp.org
