



Independent Security Operations Oversight and Assessment

*Captain Timothy Holland
PM NGEN*

23 June 2010





Independent Security Operations Oversight and Assessment

*Will Jordan
NGEN Cyber Security*

23 June 2010



The Independent Security Operations Oversight and Assessment contract provides for:





Purpose

- **ISOO&A is a capability to independently assess the security posture of the Naval Networking Environment (NNE)**
 - Will allow for independent third-party assessment
 - Provides for frequent, comprehensive security assessments and independent oversight at the network operational nodes within the enterprise
- **ISOO&A supports the need to “lead/pace information assurance threats”**



Accomplishments

- **Request For Information**
 - Released to Industry May 17, 2009
 - Responses to questions and comments were provided

- **Performance Work Statement (draft)**
 - Released to Industry for review/comment February 1, 2010
 - Comments received from Industry have been reviewed and incorporated



Security Controls

- Current and past federal CIOs and CISOs have agreed that a prioritized baseline of information security measures and controls should be established that can be continuously monitored. The initial 20 controls are published at <http://www.sans.org/critical-security-controls/guidelines.php>
- Two (2) critical IA controls withdrawn for being beyond the scope of ISOO&A
 - Application Software Security
 - Data Loss Prevention
- The following critical IA controls within the scope of ISOO&A are as follows:
 - Penetration Testing
 - Inventory of Authorized and Unauthorized Devices
 - Inventory of Authorized and Unauthorized Software
 - Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
 - Boundary Defense



Security Controls (cont)

- Maintenance, Monitoring, and Analysis of Security Audit Logs
- Controlled Use of Administrative Privileges
- Controlled Access Based on Need to Know
- Continuous Vulnerability Assessment and Remediation
- Account Monitoring and Control
- Malware Defenses
- Limitation and Control of Network Ports, Protocols, and Services
- Wireless Device Control
- Secure Network Engineering
- Incident Response Capability
- Data Restoration
- Security Skills Assessment and Appropriate Training



Additional Security Controls

- **Nine (9) Additional IA Controls (NGEN-Centric)**
 - Command and Control (C2) Tools and Processes
 - Personally Identifiable Information (PII)
 - Privacy and Security Safeguards/Security Architecture
 - Media Protection
 - Supply Chain Protection
 - Legacy Networks Security
 - Physical and Environmental Protection
 - Contingency, Continuity of Operations, and Disaster Recovery
 - Identity Management



Performance Work Statement

- **Scope**
 - DON Classified and Unclassified Networks
 - 5 primary sites
 - 51 secondary sites
- **Requirements**
 - Knowledge and Skills per DoD 8570.1
 - Minimum Secret clearance required
 - Contractor Representative within 25 miles of Washington Navy Yard
 - Services performed in 4 areas
 - Scheduling
 - Planning
 - Testing/Auditing
 - Reporting
 - 5 contract Data Requirements List (CDRL) items
 - Test/Audit Plan
 - Standard Report
 - Exception Report
 - Monthly Summary Report
 - Annual Project Report



Testing Locations

- **The ISOO&A Contractor will be expected to travel to the 5 primary test/audit sites each year, for a total of 10 trips**
 - Secondary site visits may be required as directed by the government
- **Five Primary Testing Locations**
 - Naval Station Norfolk, Norfolk, Virginia
 - Naval Air Station North Island, San Diego, California
 - Naval Station Ford Island, Pearl Harbor, Hawaii
 - Naval Station Bremerton, Bremerton, Washington
 - Naval Air Station Jacksonville, Jacksonville Florida



Scope of Testing

- **Network Devices**
 - Switches
 - Routers
 - IP addressable network components
 - Security Infrastructure
- **Application/Services Servers**
 - Provides enterprise services to end users
- **Storage**
 - Storage Area Network Servers
 - Backup Storage Servers
- **Applications (approved)**



Contract Items of Interest

- **Small Business Set Aside**
 - SeaPort-e
- **RFP anticipated release**
 - Aug 2010
 - To ensure independence, any company that serves as the ISOO&A prime contractor or as a sub to the prime contractor will be ineligible to compete for any other NGEN contract (i.e. as either a prime or subcontractor)
- **Government Furnished Information and Property**
 - Information will be provided to the successful contractor



Contract Items of Interest

Evaluation Criteria

- **Technical Approach**
 - Notional Scenario will be provided for developing a test plan as part of the technical evaluation criteria as vendors respond to the solicitation
- **Past Performance**
 - Successful individualized or team-associated past experience on an Enterprise-wide network as documented in the Contractor Performance Assessment Reporting System (CPARS), past relevant experience, and additional references as requested
- **Staffing**
 - Demonstrated ability to respond to surge or changing requirements
- **Cost**



NGEN Way Ahead

- **ISOO&A Support contract is expected to be the first competition and award in NGEN Increment 1**
 - Provides required independent security assessments on the NGEN
 - Satisfies a need of the operational community
 - Smooths the transition of network security management

- **Monitor for ISOO&A RFP release**



Questions and Answers

Submit your questions to ngen_cybersecurity@bah.com

NGEN Reference Library

www.tinyurl.com/NGENRefLibrary



Independent Security Operations Oversight and Assessment

*Captain Adam Cohan
NGEN Cyber Security*

23 June 2010





Question 1:

What is the planned ISOO&A RFP release date?

Answer:

The RFP is expected to be released in the 4th quarter of fiscal year 2010.



Question 2:

Will ISOO&A utilize the Defense Information Assurance Certification and Accreditation Process (DIACAP)?

Answer:

ISOO&A will provide Verification, Validation and Reporting (VV&R) but is separate from any Certification and Accreditation activities that may occur.



Question 3:

Is there an incumbent on this opportunity?

Answer:

No, There is no incumbent to this opportunity.



Question 4:

Will SIPRNET access and space be made available to create and transmit classified Exception Reports?

Answer:

Yes, the successful vendor will be provided access to the SIPRNET in order to create and transmit classified exception reports.



Question 5:

Does the use of the word "continual" mean 24 hours per day, 7 days per week, 365 days per year?

Answer:

No, this is not meant to be 24/7, however, the word continual means that the contractor is to provide regular, periodic audits based on government approved Test or audit plans.



Question 6:

Does the contractor have responsibility for uploading findings into a Navy or DoD Vulnerability Management System (such as the DoD VMS)?

Answer:

The ISOO&A contractor is not responsible for uploading any findings from associated test or audit into the Navy and/or DoD Vulnerability Management system.



Question 7:

Is there a requirement to employ security audit or assessment tools approved by the Government (such as a scanning tool like Retina)?

Answer:

Yes, The ISOO&A vendor will only be allowed to utilize security audit or assessment tools provided by the Government.



Question 8:

What current policy guidance will be used to develop the criteria to evaluate compliance for Supply Chain Management?

Answer:

The Committee on National Security Systems Instruction (CNSSI) 1253 or an equivalent follow on replacement technical guidance will be used to develop the criteria to evaluate compliance.



Question 9:

Is the contractor responsible for developing a new Plan of Action & Milestones or will it tie into an existing POA&M?

Answer:

There is no POA&M requirement for this support contract. ISOOA is not part of the Certification and Accreditation process.



Question 10:

How far in advance of the event will the government make the "list of approved devices and software" available to the contractor?

Answer:

Access to the list of approved devices and software will be made available to the successful contractor by the Government upon contract award.



Question 11:

Is there an Organizational Conflict of Interest (OCI) associated with the ISOO&A contract that would preclude the winning contractor from bidding on other segments of NGEN?

Answer:

Yes. The ISOOA contractor and their subcontractors, if any, must function in a completely independent manner in the performance of the ISOOA contract. The ISOOA contractors cannot be placed in a position of evaluating their own products and/or services, therefore they will not be eligible, as a prime or subcontractor from doing any NGEN work other than ISOO&A.



Independent Security Operations Oversight and Assessment

Cyber Security Industry Day

23 June 2010



PEO  **EIS**