Performance Based Statement of Work
CYBERSECURITY (CS) ANALYST
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
Naval Postgraduate School

1.0 Background/Introduction: The Naval Postgraduate School (NPS) located in Monterey, California supports the U.S. Navy, other military branches, and foreign military services with postgraduate education. Additionally, NPS provides significant research capabilities to the Department of Defense (DoD) but with the main focus on education. The Information Technology and Communication Services (ITACS) Department at NPS provides information technology (IT) support to the entire school. This includes both mission elements of research and education.

2.0 Scope: NPS provides high quality, relevant and unique advanced education and research programs that increase the combat effectiveness of the Navy, other Armed Forces of the U.S. and other partners to enhance national security. A core enabler of this mission is NPS' ability to protect and defend the school's network data and intellectual property from unauthorized use. This is a very challenging requirement because of the highly available network that supports multiple, complex requirements, including collaborative partnerships with other DoD entities, advanced research conducted by NPS faculty, membership in a number of regional and national higher education networks, cutting edge research in networking, and many other initiatives. In order to better protect the dual mission of providing higher education on the one hand, and advanced research on the other, NPS needs to improve its network security, prevent intrusions, understand the normal operations of network traffic to better defense the resources of NPS networking. All of this should be completed in a manner consistent with its mission, while also meeting the security requirements unique to the Navy and DoD.

The scope of this contract is to provide CND service support and expertise in protecting NPS data and networks (EDU, DREN, and SIPRNet) with a focus on incident response and handling. Additionally, the CS Analyst shall coordinate with the Defense Language Institute-Foreign Language Center (DLI-FLC) on any incidents identified by Navy Cyberdefense Operations Command (NCDOC) or the High Performance Computing-Computer Emergency Response Team (HPC-CERT) that are attributed to DLI-FLC activity.

3.0 Tasks:

The contractor shall perform the following task as follows:

3.1 Receives and analyzes network alerts from various sources within the enclave and determines possible causes of such alerts.
3.2 Coordinates with enclave Cybersecurity staff to validate network alerts.
3.3 Performs analysis of log files from a variety of sources within the enclave, to include individual host logs, network traffic logs, firewall logs, and intrusion detection system logs.
3.4 Characterizes and analyzes network traffic to identify anomalous activity and potential threats to network resources.
3.5 Monitors external data sources (e.g. Cybersecurity vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Cybersecurity threat condition and determine which security issues may have an impact on the enclave.
3.6 Assists in the construction of signatures that can be implemented in Cybersecurity network tools in response to new or observed threats within the enclave.
3.7 Performs event correlation using information gathered from a variety of sources within the enclave to gain situational awareness and determine the effectiveness of an observed attack.
3.8 Notifies Cybersecurity leadership, Cybersecurity incident responders, and other Cybersecurity team members of suspected Cybersecurity incidents and articulates the event's history, status, and potential impact for further action.
3.9 Prepares incident management documentation in an accurate and professional manner
3.10 Participates in daily, weekly, and twice monthly meetings to provide status updates and align goals.

4.0 Deliverables:

The contractor shall be responsible for providing the following deliverables:

4.1 Completed documentation of cybersecurity incidents from discovery to closure. Information will include, but not be limited to, the following elements:
- 4.1.1 Incident category
- 4.1.2 Source IP(s) of incident
- 4.1.3 Destination IP(s) of incident
- 4.1.4 Incident details
- 4.1.5 Actions taken to resolve / close incident

4.1.6 Applicable log files
4.1.7 Population of executive summary information to ensure accuracy of incident executive report

4.2 Monthly status report covering total number of incidents managed, number of incidents opened and number of incidents closed. Additional information shall include:
4.2.1 Other JIRA issues opened and / or closed
4.2.2 Other significant accomplishments during the month

4.3 Twice monthly accomplishment reports, which will be submitted via the NPS Wiki. Reports will include:
4.3.1 Top 3-5 accomplishments for the two week period
4.3.2 Other JIRA issues opened and / or closed
4.3.3 Items not accomplished; reasons for non-accomplishment; support / assistance required

4.4 Lead the Bi-weekly incident brief to be delivered to the NPS CIO and/or Deputy CIO. Brief will include:
4.4.1 Incident workload for last year, year to date, last 30 days, and last 2 weeks
4.4.2 Abuse workload for last year, year to date, last 30 days, and last 2 weeks
4.4.3 Breakdown of compromised and not-compromised, DMZ and Internal hosts for last 2 weeks, last 30 days and year to date
4.4.4 Major incidents and unresolved incidents

Performance Measurement - Quality Assurance Plan

Task	Deliverable that will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
3.1 – 3.10	4.1 Incident Documentation	Information will be documented in JIRA NLT 4 hours after external report received or internal event discovered.	Electronic submission via JIRA workflow management system and Cybersecurity wiki.	As incidents occur.
3.1 – 3.10	4.2 Monthly Status Report	At least one to two pages in length covering activity previously taken.	Electronic submission via private server or reporting dashboard via the Cybersecurity team wiki.	10th calendar day of each month.
3.1-3.10	4.3 Twice Monthly Accomplishments Report	Report will be documented on the wiki by COB the day prior to the accomplishments meeting and link to other related efforts documented in JIRA.	Electronic submission via via the Cybersecurity team wiki	Twice per month on Friday in accordance with Cybersecurity team schedule.
3.1-3.10	4.4 Bi-weekly incident brief	Brief will provide ITACS management with appropriate level of situational awareness on cybersecurity incidents – specifically, what happened, impact to NPS mission and any noticeable trends in cyber incidents.	Electronic submission via private server or reporting dashboard via the Cybersecurity team wiki	Twice per month on Friday in accordance with Cybersecurity team schedule.

If performance falls below the AQL defined above, the Contracting Officer's Representative (COR) shall document the instance(s), coordinate with the Contracting Officer and advise the Contractor. The Contractor will be requested to review the documentation and provide a written response on how performance will be corrected in the future. Re-performance of any work for failure to perform in accordance with the specified AQL or task requirement shall be completed at the Contractor's own expense and at no additional cost to the Government.

5.0 Minimum Technical Requirements (also reference FAR 39 attachment):

5.1 Requires three to five years of information security experience. Must possess a background in incident handling, response and intrusion detection (IDS) experience. Ability to interpret IDS signatures, firewall alerts, and anti-virus alerts and experience directing the remediation of incidents (intrusions, infections, misuse, etc). Knowledge of TCP/IP networking, switches, routers, firewalls, VPN, and encryption is required.

5.2 Ability to perform daily analytical actions in the performance of responding to incidents, identifying appropriate mitigation actions, identifying proper escalation procedures, and analyzing data collection and reporting requirements. Assist in developing, managing, communicating, and implementing an incident response program. It is preferred that this person be a current Certified Information Systems Security Professional (CISSP), but they must minimally be certified as a security professional at the DoD 8570 level II Information Assurance Technical (IAT) certification such as CompTIA's Security+.

6.0 Period of Performance: Period of performance is twelve months from date of award.

7.0 Place of Performance: The work will be performed at Naval Postgraduate School, Monterey, CA 93943.

8.0 Government Furnished Property: The government shall provide appropriate office space, supplies and equipment to perform tasks at NPS. Any Government-provided property and information shall be used for official Government business only. This includes phone, desktop computer, desk, and physical workspace.

9.0 Work Week and Hours of Operation:

The Contractor shall provide services during normal working hours excluding federal holidays. Normal working hours are 0730-1630, Monday through Friday, unless requirements dictate otherwise. Exceptions can be permitted by the COR upon request and at the COR's discretion.

Following is a list of holidays observed by the Government.

Name of Holiday	Time of Observance
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity

10.0 Travel: No travel is anticipated at this time, but there may be circumstances where travel may be required. If travel is required, it will be in accordance with the Joint Travel Regulations (JTR) and will be reimbursed by the government on an as-incurred basis.

11.0 Security Requirements: Proper performance of this contract will require classified work to take place at government facilities. All contractor personnel performing under this contract must have a current security investigation and must be eligible for access to Secret information. The prime contractor must have an active Secret or above Facility Clearance. The security requirements are in accordance with the attached DD254. Contractor Key Personnel must be U.S. Citizens.

12.0 Privacy Act Statement:

"Pursuant to Title 5 United States Code 552a(m)(l), the contractor and all employees of the contractor working under this contract are required to comply with the requirements of 5 U.S.C. 552a ("The Privacy Act of 1974")."

13.0 Identification of Contractor Employees:

In accordance with DFAR 211.106, there shall be a clear distinction between Government employees and service contractor employees. Service contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel. Contractor personnel will be required to obtain and wear badges or other visible identification for meetings with Government personnel to provide a clear distinction between service contractor employees and Government personnel. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

14.0 Non-Personal Services Statement:

Contractor employees performing services under this order will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management will insure that employees properly comply with the performance work standards outlined in the SOW. Contractor employees will perform their duties independent of, and without the supervision of, any Government official or other Defense Contractor. The tasks, duties, and responsibilities set forth in the task order may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government will control access to the facility and will perform the inspection and acceptance of the completed work.

15.0 Transition Plan.

It is essential to the Government that services required under this PWS are performed without interruption. Consequently, it is imperative that transition to full contract performance be accomplished in a well-planned, orderly, and efficient manner. The transition period shall begin 30 days prior to full contract performance as required by the solicitation/contract, which is anticipated to be 21 August 2015. The purpose of this orientation is primarily to:

- Observe work accomplished by current contractor personnel.
- Obtain security clearances.
- Accomplish necessary training of contractor employees.
- Establish workstations.
- Transfer Government Furnished Property.

16.0 Transition Activities.

At the conclusion of any performance period, including option periods or extensions, the services provided under this PWS may be awarded to another contractor. The contractor in place shall be required to assist in the transition activities.

17.0 Points of Contact:

NPS Technical POC:
Bob Goodwin, CISSP
Director of Cybersecurity
Information Technology and Communications Services (ITACS)
U.S. Naval Postgraduate School
555 Dyer Road, Monterey, CA 93943
DSN: 312.756.1048
Comm: 831.656.1048
rdgoodwi1@nps.edu

NPS POC for Acceptance of Deliverables: Same as TPOC.

NPS Financial POC: Dee Morais