

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

STATEMENT OF WORK

Background / Introduction

The Naval Postgraduate School (NPS) located in Monterey, CA supports the U.S. Navy, other U.S. military branches, DoD and other government agencies, and foreign military services with postgraduate education for personnel. Additionally, NPS provides significant research capabilities to the DoD and other government agencies. The Information Technology And Communications Services (ITACS) Department at NPS provides information technology (IT) support to the entire University.

NPS has multiple networks operated by ITACS for use in the execution of its mission. Two of these networks require the renewal of their tri-annual Authority to Operate (ATO). These networks are:

Defense Research and Engineering Network (DREN): the U. S. DoD's research and engineering computer network. It is a high speed, high capacity, low latency nationwide computer network for computational scientific research, engineering, and testing in support of the DoD's Science and Technology and Test and Evaluation communities.

Secret Internet Protocol Router Network (SIPRNet): the secret component of the DoDIN. It is a system of interconnected computer networks used for the DoD and Department of State to transmit classified information up to and including SECRET.

The NPS CIO will oversee the security testing, validation, and risk determination that will be submitted with accreditation packages to:

- The Navy Authorizing Official (AO) via the AO Designated Representative (AODR) process for the DREN.
- The Navy Certifying Authority for validation and submission to the Navy Operational Designated Accrediting Authority (ODAA) for the SIPRNet.

This assessment effort will be done using the DoD Information Certification and Accreditation Program (DIACAP) process to attain 30 month ATOs per recent Navy guidance for both networks.

Scope

The scope of this contract is to provide separate security testing and evaluation (ST&E) services in support of the separate certifications of the NPS DREN and SIPRNet networks in accordance with current Navy and DoD accreditation requirements, i.e., the DIACAP. NPS assumes the roles of "Validator" and "Certifying Authority" for the DREN assessment and as Echelon II for the STBL assessment. The contractor will only

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA

assume the role of tester for both network assessments. The DREN ST&E work will be conducted first followed by ST&E work for the SIPRNet.

ATOs or IATOs will be granted by the ODAA in accordance with the following references (available upon request):

1. OPNAVINST 5239.1C
2. DoD Instruction 8501.01 of 28 November 2007
3. CJCSI 6211.02D of 24 January 2012
4. CJCSI 6510.01F of 9 February 2011
5. DoD Instruction 8500.2 of 6 February 2003
6. DoD Directive 8500.01E of 23 April 2007
7. DON CIO WASHINGTON DC 081605Z Jan 09
8. DoD Directive 5230.20 of 22 June 05
9. DoD Instruction 8420.01 of 3 Nov 09
10. DON CIO memo of 6 December 12
11. CTF 1010 091600Z Nov 12 (ALCOM 182/12)

The vendor shall test, evaluate, and document the IA controls and system security configurations for:

DREN – Mission Assurance Category (MAC) II Sensitive
SIPRNet – Mission Assurance Category (MAC) III, Classified SECRET up to
NATO SECRET

The vendor shall determine and document remediation activities and mitigating controls that address all findings for components of the DREN and SIPRNet networks, respectively.

ALL WORK MUST BE ACCOMPLISHED ON SITE AT NPS.

NO WORK MAY BE COMPLETED REMOTELY.

Tasks

The vendor shall perform the following tasks for each network as follows:

1. Complete manual and automated security testing and reviews of the technologies documented in Table 1, Technologies for Security Test & Evaluation (DREN) and Table 2, Technologies for Security Test & Evaluation (SIPRNet) against current DoD Security Technical Implementation Guides (STIGs), DoD Security Requirements Guidelines (SRG), or Industry recommended best security practices.
 - a. Conduct automated reviews using Security Requirements Review (SRR) scripts provided by DISA, customer configuration review

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA

scripts, or third party configuration review tools the output of which will be documented and reviewed with NPS.

- b. Conduct manual reviews using DISA STIGs, SRGs, and Checklists and / or Industry best practices the output of which will be documented and reviewed with NPS. This may require over the shoulder review of systems as well as face-to-face interviews with system administrators. Privileged access may not be provided to the vendor.
2. Complete and document the test and the evaluation procedures to test the MAC Level II Sensitive DIACAP IA controls for DREN as documented in Table 3: NPS DREN IA Controls.
3. Complete and document the test and the evaluation procedures to test the MAC Level III Classified SECRET up to NATO SECRET DIACAP IA controls for SIPRNet as documented in Table 4: NPS SIPRNet IA Controls.
4. Test, evaluate and document the overall network security vulnerability scans testing results based on periodic REM Retina and / or ACAS vulnerability scans of the DREN and SIPRNet.
5. Document and develop a separate POAM for all outstanding findings whose risk level is CAT 1 (high), CAT 2 (medium) and CAT 3 (low) for each network.
6. Participate in daily and weekly meetings, and situational meetings as needed, to provide status updates and align goals with the efforts in scope. Conduct daily coordination with the ITACS staff and document content on the ITACS wiki and or JIRA for the DREN, and a designated shared classified drive for the SIPRNet. Conduct weekly status meetings with ITACS leadership and document in the ITACS wiki and or JIRA or SIPRNet shared classified drive as appropriate. Attend collaboration meetings with the Navy CA, the ODAA representative and NPS management.

Deliverables

The vendor shall be responsible for preparing deliverables listed on the following pages in support of the tasks identified in this SOW.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
1.a	Automated Review of Technologies, Security, Test, and Evaluation for the DREN and the SIPRNet.	Review documentation is based on the Security Requirements Review script provided by DISA, custom review scripts, or approved 3 rd party configuration review tools and contains the following information: <ul style="list-style-type: none"> • System Identification by IP address and fully qualified domain name; • Media Access Control address; • Operating System version & patch level; • Validation procedures: planned & accomplished • Results: expected and actual • Findings and observations; • Risk Level: Original and residual; • Mapping to appropriate DoD IA Controls via IA Control numbers. 	Review by NPS Information System Security Manager	Upon Completion within 60 days of contract award.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
1.b	Manual Review of Technologies, Security, Test, and Evaluation for the DREN and the SIPRNet.	Review documentation is based on DISA STIGs, security requirements guidelines, and checklists / industry best practices; documentation includes: <ul style="list-style-type: none"> • System Identification by IP address and fully qualified domain name; • Media Access Control address; • Operating System version & patch level; • Validation procedures: planned & accomplished • Results: expected and actual • Findings and observations; • Risk Level: Original and residual; Mapping to appropriate DoD IA Controls via IA Control numbers. Testing documentation will be completed within the JIRA project and the Project wiki for the DREN and designated shared drive for SIPRNet	Review by NPS Information System Security Manager	Upon Completion within 60 days of contract award.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
2	Validation Procedures Documentation (DREN).	Documentation contains the following: <ul style="list-style-type: none"> • Control number, name, description and subject area • Threat and vulnerability countermeasures • General implementation guidance • System-specific guidance resources • Impact code • Validation procedure number, name, objective, preparation & script • Expected and actual results • Findings and observations, to include finding ID, original risk level, and residual risk level Testing documentation will be completed within the JIRA project and the Project wiki.	Review by NPS Information System Security Manager	Within two weeks upon completion of Tasks 1.a and 1.b

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
3	Validation Procedures Documentation (SIPRNet).	Documentation contains the following: <ul style="list-style-type: none"> • Control number, name, description and subject area • Threat and vulnerability countermeasures • General implementation guidance • System-specific guidance resources • Impact code • Validation procedure number, name, objective, preparation & script • Expected and actual results • Findings and observations, to include finding ID, original risk level, and residual risk level Testing documentation will be completed within the designated SIPRNET shared classified drive.	Review by NPS Information System Security Manager	Within two weeks upon completion of Tasks 1.a and 1.b

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUTATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
4	Network Vulnerability Scan Documentation	<p>Vulnerability scan test results are based on REM Retina and ACAS vulnerability scans of the DREN and SIPRNet and documentation contains the following:</p> <ul style="list-style-type: none"> • Vulnerability ID, description, System Identification by IP address and fully qualified domain name; • Media Access Control address; • Operating System version & patch level; • Validation procedures: planned & accomplished • Results: expected and actual • Findings and observations; • Risk Level: Original and residual; • Mapping to appropriate DoD IA Controls via IA Control numbers <p>Testing documentation will be completed within the JIRA project and the Project wiki for the DREN and designated shared drive for SIPRNet.</p>	Review by NPS Information System Security Manager	Within two weeks upon completion of Tasks 1.1 and 1.b
5	Plan of Action and Milestones	<p>POAM assigns a finding ID, lists the required action, identifies responsible personnel and resources required to address the finding (time, budget, expertise), and projects an expected date of resolution for all findings identified in tasks 1 – 4.</p> <p>Testing documentation will be completed within the JIRA project and the Project wiki for the DREN and designated shared drive for SIPRNet.</p>	Review by NPS Information System Security Manager	Within two weeks upon completion of Tasks 2 and 4 for the DREN and 3 and 4 for the SIPRNet.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUTATE SCHOOL
 MONTEREY, CA

Task	What will be inspected	Acceptable Quality Level (AQL)	Method	Frequency
6	Meeting Participation	Accurate documentation is maintained on the NPS Wiki, JIRA, or reporting dashboard, for the DREN, and reporting dashboard and designated shared drive for the SIPRNet. Status is communicated at daily, weekly, and situational meetings.	Review by NPS Information System Security Manager	Continuous throughout the PoP.

The surveillance method for the deliverables listed above will be personal observation at NPS. If performance fall below the AQL defined above, the Contracting Officer’s Representative (COR) shall document the instance(s), coordinate with the Contracting Officer (KO) and advise the vendor. The vendor will be requested to review the documentation and provide a written response on how performance will be corrected in the future. 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.

Period of Performance

Work will commence upon award of contract for no more than 12 weeks: 4 weeks for the DREN and 8 weeks for the SIPRNet, with specific schedules to be determined shortly after contract award.

Place of Performance

DREN – Ingersoll Hall, Room 148/149, NPS Monterey, CA and various locations around campus.

SIPRNet – Glasgow Hall, Systems Technology Battle Lab (STBL), NPS Monterey, CA and various locations around campus.

ALL WORK MUST BE ACCOMPLISHED ON SITE AT NPS.

NO WORK MAY BE COMPLETED REMOTELY.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

Work Week and Hours of Operation

The vendor shall provide services during normal working hours excluding federal holidays on location at NPS. Normal working hours are 0800 – 1630 PT, Monday through Friday, unless requirements dictate otherwise. Exceptions can be permitted by the COR upon request and at the COR's sole discretion.

Work required on site at NPS shall be performed by the Contractor, as required.

Holidays observed by the Government

<u>Name of Holiday</u>	<u>Time of Observance</u>
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.

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. Any applicable documents that are authorized for use in performance of these services shall be provided, in accordance with security and contract terms and conditions.

Travel

Travel is not expected for this contract.

Classification

Access to sensitive information is required up to and including PII and FOR OFFICIAL USE ONLY for the DREN and SECRET for the SIPRNet. Contractor must be eligible for or have a DoD CAC that is valid the entire period of the performance and must have a current NACLIC investigation per DoD requirements of an IT level 2 designated position. Contractor shall maintain eligibility for a US DoD SECRET clearance during the entire period of performance.

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUTATE SCHOOL
 MONTEREY, CA

Table 1: Technologies for Security, Test, and Evaluation (DREN)

Function	Make	Model	STIGs and SRGs (as available at the start of the contract PoP)
Workstation OS	Microsoft	Windows 7	Windows 7 STIG Best practices
Web Browser	Microsoft	Microsoft Internet Explorer	MS IE STIG
Office Suite	Microsoft	Microsoft Office	MS Office STIG
Server OS (member)	Microsoft	Windows 2003 and 2008 R2	Windows 2003 2008 R2 STIG
Server OS (Domain Controller)	Microsoft	Windows 2008 R2	Windows 2008 R2 DC STIG
.net	Microsoft	Microsoft .Net Framework	MS .Net Framework STIG
Server OS	RedHat	Enterprise Linux v5	Red Hat 5 STIG Benchmark Red Hat 5 Manual STIG
Server OS	RedHat	Enterprise Linux v6	Red Hat 6 STIG Benchmark
Directory Service	Microsoft	Active Directory Service 2008	AD Service 2008 STIG
Database	Oracle	MySQL 5.6	N/A
Router	Brocade	NetIron MLXe-4 Router	Router SRG
Router	Juniper	EX3200	Network perimeter router L3 switch router SRG
Switch (L2)	Brocade	FESx448	Network L2 Switch STIG
Switch (L2)	Brocade	ICX 6430 and 6450 series	Network L2 Switch STIG
DNS (internal)	Microsoft	Windows 2008 R2	DNS Security Checklist DNS STIG
DNS (external)	BIND	BIND on UNIX	DNS Security Checklist DNS STIG
Firewall	Juniper	Netscreen SSG-550M	Firewall SRG
VPN	Cisco	ASA 5540	IPSEC VPN Gateway STIG
Intrusion Detection and Prevention	General	Policy	SRG
Network Security	General	Policy	SRG
Physical Security	General	Policy	Traditional Security Checklist
Web Policy	General	Policy	STIG
Wireless	General	Policy	General Wireless Policy STIG
DoDNet Router	NetIron	NetIron MLX 8	Router SRG
DoDNet Switch	Brocade	Brocade FGS624P	Network L2 Switch STIG
Secure VTC	Tandberg		

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUATE SCHOOL
 MONTEREY, CA

Table 2: Technologies for Security, Test, and Evaluation (SIPRNet)

Function	Make	Model	STIGs and SRGs (as available at the start of the contract PoP)
Workstation OS	Microsoft	Windows 7	Windows 7 STIG
Web Browser	Microsoft	Microsoft Internet Explorer	MS IE STIG
Office Suite	Microsoft	Microsoft Office	MS Office STIG
Antivirus	HBSS	Endpoint Protection	HBSS STIG
Server OS (member)	Microsoft	Windows 2003 /2008 R2	Windows 2003 / 2008 R2 STIG
Server OS (Domain Controller)	Microsoft	Windows 2008 R2	Windows 2008 R2 DC STIG
.net	Microsoft	Microsoft .Net Framework	MS .Net Framework STIG
Server OS	RedHat	Enterprise Linux v5	Red Hat 5 STIG Benchmark Red Hat 5 Manual STIG
Server OS	RedHat	Enterprise Linux v6	Red Hat 6 STIG Benchmark
Directory Service	Microsoft	Active Directory Domain	AD Domain STIG
Directory Service	Microsoft	Active Directory Service 2008	AD Service 2008 STIG
Database	Microsoft	SQL 2008 R2	SQL Server 2008 Database Security Checklist
Database	Microsoft	SQL 2005	SQL Server 2005 Database Security Checklist
Perimeter Router	Cisco	3800	Network Perimeter Router L3 switch Router SRG
Switch (L2)	Cisco	Catalyst 3750G	Network L2 Switch STIG
Firewall	Cisco	PIX	Firewall SRG
DNS (internal)	Microsoft	Windows 2008 R2	DNS Security Checklist DNS STIG
DNS (external)	BIND	BIND on UNIX	DNS Security Checklist DNS STIG
Mail	Microsoft	Exchange 2007 Client Access Server	Exchange 2007 Client Access Server
Mail	Microsoft	Exchange 2007 Edge Transport Server	Exchange 2007 Edge Transport Server
Mail	Microsoft	Exchange 2007 Hub Transport Server	Exchange 2007 Hub Transport Server
Mail	Microsoft	Exchange 2007 Mailbox Server STIG	Exchange 2007 Mailbox Server STIG
Intrusion Detection and Prevention	General	Policy	SRG
Network Security	General	Policy	SRG
Physical Security	General	Policy	Traditional Security Checklist
Web Policy	General	Policy	STIG

SECURITY TEST AND EVALUATION (ST&E) SERVICES
 INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
 NAVAL POSTGRADUTATE SCHOOL
 MONTEREY, CA

Table 3: NPS DREN IA Controls

COAS-2	Alternate Site Designation (High)
COBR-1	Protection of Backup and Restoration Assets (High)
CODB-2	Data Backup Procedures (Medium)
CODP-2	Disaster and Recovery Planning (Medium)
COEB-2	Enclave Boundary Defense (Medium)
COED-1	Scheduled Exercises and Drills (Low)
COEF-2	Identification of Essential Functions (Medium)
COMS-2	Maintenance Support (Medium)
COPS-2	Power Supply (Medium)
COSP-1	Spares and Parts (Medium)
COSW-1	Backup Copies of Critical SW (High)
COTR-1	Trusted Recovery (High)
DCAR-1	Procedural Review (Medium)
DCAS-1	Acquisition Standards (High)
DCBP-1	Best Security Practices (Medium)
DCCB-2	Control Board (Medium)
DCCS-2	Configuration Specifications (High)
DCCT-1	Compliance Testing (Medium)
DCDS-1	Dedicated IA Services (Medium)
DCFA-1	Functional Architecture for AIS Applications (Medium)
DCHW-1	HW Baseline (High)
DCID-1	Interconnection Documentation (High)
DCII-1	IA Impact Assessment (Medium)
DCIT-1	IA for IT Services (High)
DCMC-1	Mobile Code (Medium)
DCNR-1	Non-repudiation (Medium)
DCPA-1	Partitioning the Application (Low)
DCPB-1	IA Program and Budget (High)
DCPD-1	Public Domain Software Controls (Medium)
DCPP-1	Ports, Protocols, and Services (Medium)
DCPR-1	CM Process (High)
DCSD-1	IA Documentation (High)
DCSL-1	System Library Management Controls (Medium)
DCSP-1	Security Support Structure Partitioning (Medium)
DCSQ-1	Software Quality (Medium)
DCSR-2	Specified Robustness – Medium (High)
DCSS-2	System State Changes (Medium)
DCSW-1	SW Baseline (High)
EBBD-2	Boundary Defense (Medium)
EBCR-1	Connection Rules (Medium)

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

EBPW-1	Public WAN Connection (High)
EBRP-1	Remote Access for Privileged Functions (High)
EBRU-1	Remote Access for User Functions (High)
EBVC-1	VPN Controls (Medium)
ECAD-1	Affiliation Display (Medium)
ECAN-1	Access for Need-to-Know (High)
ECAR-2	Audit Record Content – Sensitive Systems (Medium)
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting (Low)
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting (Medium)
ECCD-2	Changes to Data (High)
ECCR-1	Encryption for Confidentiality (Data at Rest) (Low)
ECCT-1	Encryption for Confidentiality (Data at Transmit) (Medium)
ECDC-1	Data Change Controls (Medium)
ECIC-1	Interconnections among DoD Systems and Enclaves (High)
ECID-1	Host Based IDS (Medium)
ECIM-1	Instant Messaging (Medium)
ECLO-1	Logon (Medium)
ECLP-1	Least Privilege (High)
ECML-1	Marking and Labeling (High)
ECMT-1	Conformance Monitoring and Testing (Medium)
ECND-2	Network Device Controls (Medium)
ECNK-1	Encryption for Need-To-Know (Medium)
ECPA-1	Privileged Account Control (High)
ECPC-2	Production Code Change Controls (Medium)
ECRC-1	Resource Control (Medium)
ECRG-1	Audit Reduction and Report Generation (Low)
ECRR-1	Audit Record Retention (Medium)
ECSC-1	Security Configuration Compliance (High)
ECSD-2	Software Development Change Controls (High)
ECTB-1	Audit Trail Backup (Medium)
ECTC-1	Tempest Controls (High)
ECTM-2	Transmission Integrity Controls (High)
ECTP-1	Audit Trail Protection (Medium)
ECVI-1	Voice-over-IP (VoIP) Protection (Medium)
ECVP-1	Virus Protection (High)
ECWM-1	Warning Message (High)
ECWN-1	Wireless Computing and Network (High)
IAAC-1	Account Control (High)
IAGA-1	Group Authentication (Medium)
IAIA-1	Individual Identification and Authentication (High)
IAKM-2	Key Management (Medium)

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

IATS-2	Token and Certificate Standards (Medium)
PECF-1	Access to Computing Facilities (High)
PECS-1	Clearing and Sanitizing (High)
PEDI-1	Data Interception (High)
PEEL-2	Emergency Lighting (Medium)
PEFD-2	Fire Detection (High)
PEFI-1	Fire Inspection (Medium)
PEFS-2	Fire Suppression (High)
PEHC-2	Humidity Controls (Medium)
PEMS-1	Master Power Switch (High)
PEPF-1	Physical Protection of Facilities (High)
PEPS-1	Physical Security Testing (Low)
PESL-1	Screen Lock (Medium)
PESP-1	Workplace Security Procedures (Medium)
PESS-1	Storage (High)
PETC-2	Temperature Controls (Medium)
PETN-1	Environmental Control Training (Low)
PEVC-1	Visitor Control to Computing Facilities (High)
PEVR-1	Voltage Regulators (High)
PRAS-1	Access to Information (High)
PRMP-1	Maintenance Personnel (High)
PRNK-1	Access to Need-to-Know Information (High)
PRRB-1	Security Rules of Behavior or Acceptable Use Policy (High)
PRTN-1	Information Assurance Training (High)
VIIR-1	Incident Response Planning (Medium)
VIVM-1	Vulnerability Management (High)

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

Table 4: NPS SIPRNet IA Controls

COAS-1	Alternate Site Designation (Medium)
COBR-1	Protection of Backup and Restoration Assets (High)
CODB-1	Data Backup Procedures (Low)
CODP-1	Disaster and Recovery Planning (Low)
COEB-1	Enclave Boundary Defense (Medium)
COED-1	Scheduled Exercises and Drills (Low)
COEF-1	Identification of Essential Functions ((Low)
COMS-1	Maintenance Support (Medium)
COPS-1	Power Supply (Low)
COSP-1	Spares and Parts (Medium)
COSW-1	Backup Copies of Critical SW (High)
COTR-1	Trusted Recovery (High)
DCAR-1	Procedural Review (Medium)
DCAS-1	Acquisition Standards (High)
DCBP-1	Best Security Practices (Medium)
DCCB-1	Control Board (Low)
DCCS-1	Configuration Specifications (High)
DCCT-1	Compliance Testing (Medium)
DCDS-1	Dedicated IA Services (Medium)
DCFA-1	Functional Architecture for AIS Applications (Medium)
DCHW-1	HW Baseline (High)
DCID-1	Interconnection Documentation (High)
DCII-1	IA Impact Assessment (Medium)
DCIT-1	IA for IT Services (High)
DCMC-1	Mobile Code (Medium)
DCNR-1	Non-repudiation (Medium)
DCPD-1	Public Domain Software Controls (Medium)
DCPP-1	Ports, Protocols, and Services (Medium)
DCPR-1	CM Process (High)
DCSD-1	IA Documentation (High)
DCSL-1	System Library Management Controls (Medium)
DCSQ-1	Software Quality (Medium)
DCSR-3	Specified Robustness – High (High)
DCSS-1	System State Changes (High)
DCSS-2	System State Changes (Medium)
DCSW-1	SW Baseline (High)
EBBD-3	Boundary Defense (Low)
EBCR-1	Connection Rules (Medium)
EBRP-1	Remote Access for Privileged Functions (High)
EBRU-1	Remote Access for User Functions (High)

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUTATE SCHOOL
MONTEREY, CA

EBVC-1	VPN Controls (Medium)
ECAD-1	Affiliation Display (Medium)
ECAN-1	Access for Need-to-Know (High)
ECAR-3	Audit Record Content – Classified Systems Audit of Security Label Changes (High)
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting (Low)
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting (Medium)
ECCD-1	Changes to Data (Medium)
ECCD-2	Changes to Data (High)
ECCM-1	COMSEC (High)
ECCR-2	Encryption for Confidentiality (Data at Rest) (Medium)
ECCR-3	Encryption for Confidentiality (Data at Rest) (High)
ECCT-2	Encryption for Confidentiality (Data at Transmit) (High)
ECIC-1	Interconnections among DoD Systems and Enclaves (High)
ECIM-1	Instant Messaging (Medium)
ECLC-1	Audit Record Content – Classified Systems Audit of Security Label Changes (Low)
ECLO-2	Logon (Medium)
ECLP-1	Least Privilege (High)
ECML-1	Marking and Labeling (High)
ECMT-2	Conformance Testing (High)
ECND-1	Network Device Controls (Low)
ECNK-1	Encryption for Need-To-Know (Medium)
ECNK-2	Encryption for Need-To-Know (Medium)
ECPA-1	Privileged Account Control (High)
ECPC-1	Production Code Change Controls (Medium)
ECRC-1	Resource Control (Medium)
ECRG-1	Audit Reduction and Report Generation (Low)
ECRR-1	Audit Record Retention (Medium)
ECSC-1	Security Configuration Compliance (High)
ECSD-1	Software Development Change Controls (Medium)
ECTB-1	Audit Trail Backup (Medium)
ECTC-1	Tempest Controls (High)
ECTM-1	Transmission Integrity Controls (Medium)
ECTP-1	Audit Trail Protection (Medium)
ECVI-1	Voice-over-IP (VoIP) Protection (Medium)
ECVP-1	Virus Protection (High)
ECWM-1	Warning Message (High)
ECWN-1	Wireless Computing and Network (High)
IAAC-1	Account Control (High)
IAGA-1	Group Authentication (Medium)
IAIA-1	Individual I & A (High)
IAIA-2	Individual Identification and Authentication (High)
IAKM-1	Key Management (Medium)

SECURITY TEST AND EVALUATION (ST&E) SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA

IAKM-3	Key Management (Medium)
IATS-1	Token and Certificate Standards (Medium)
PECF-2	Access to Computing Facilities (High)
PECS-2	Clearing and Sanitizing (High)
PEDD-1	Destruction (High)
PEDI-1	Data Interception (High)
PEEL-1	Emergency Lighting (Low)
PEFD-1	Fire Detection (High)
PEFI-1	Fire Inspection (Medium)
PEFS-1	Fire Suppression (Medium)
PEHC-1	Humidity Controls (Medium)
PEMS-1	Master Power Switch (High)
PEPF-2	Physical Protection of Facilities (High)
PEPS-1	Physical Security Testing (Low)
PESL-1	Screen Lock (Medium)
PESP-1	Workplace Security Procedures (Medium)
PESS-1	Storage (Medium)
PETC-1	Temperature Controls (Low)
PETN-1	Environmental Control Training (Low)
PEVC-1	Visitor Control to Computing Facilities (High)
PEVR-1	Voltage Regulators (High)
PRAS-2	Access to Information (High)
PRMP-2	Maintenance Personnel (High)
PRNK-1	Access to Need-to-Know Information (High)
PRRB-1	Security Rules of Behavior or Acceptable Use Policy (High)
PRTN-1	Information Assurance Training (High)
VIIR-1	Incident Response Planning (Medium)
VIVM-1	Vulnerability Management (High)