

**UNCLASSIFIED**

***DIL***

17 May 2012

STOCII-14-KOP-003

Enc 9-DIL SOP-4.0

**PEO STRI DIGITAL INTEGRATION LABORATORY**

**(DIL)**

**STANDARD OPERATING PROCEDURE**

**(SOP)**



**DIL SOP**

**Version 4.0**

**18 May 2012**

Prepared by:

PEO STRI PM WTL

12000 Research Pkwy, Suite 300

Orlando, FL 32825

---

**UNCLASSIFIED  
FOR OFFICIAL USE ONLY**



**Table of Contents**

**Table of Contents** ..... 3

**List of Appendixes and Attachments** ..... 4

**1.0 References** ..... 5

**1.0.1 DoD Directive 5220.20-M National Industrial Security Program Operating Manual (NISPOM)** ..... 5

**1.0.2 PEO STRI Security Standard Operating Procedures** ..... 5

**1.0.3 Central Texas Army Interoperability Program Standard Operating Procedures** ..... 5

**1.1 Physical Security** ..... 5

**1.2 Procedures For Sending Visit Access Requests (VAR) to the PEO STRI Joint Development Integration Facility (JDIF)**..... 5

**1.3 Procedures for Non-Permenant Visitors Granted JDIF Access** ..... 6

**1.4 PEO STRI JDIF SECRET Lab Uncleared Visitor Policy** ..... 6

**1.5 Shipping Classified Material**..... 10

**1.6 PEO STRI JDIF Opening/Closing Security Check** ..... 11

**2.0 Computer and Network Security Procedures** ..... 11

**2.1 DoD Information System (IS) User Agreement**..... 11

**2.2 Incoming Media** ..... 11

**2.3 Outgoing Media**..... 11

**2.4 Information Assurance Vulnerability Management (IAVM)**..... 12

**2.4.1 IAVM Applicability and Scope**..... 12

**2.4.2 DIL Quarterly IAVA Updates** ..... 13

**2.4.3 Procedures for Applying Patches** ..... 13

**3.0 DIL Army Mission Command (MC) System Integration Support** ..... 13

**3.1 DIL Support Request Form** ..... 13

**3.2 Request for Loan of MC Hardware (HW) and Software (SW)**..... 13

**4.0 Formal Army Interoperability Certification (AIC) Support** ..... 13

**4.1 Responsibilities of the System Under Test (SUT)** ..... 14

**4.2 DIL Software Baseline and Network Architecture**..... 14

**5.0 DIL MC Integration Support** ..... 14

**5.1 Pre-Event Meeting** ..... 14

**5.2 Post Event Meeting (AAR)** ..... 14

**5.3 Stand-Alone Integration**..... 14

**6.0 Firewall and Intrusion Detection System (IDS)** ..... 15

**Appendix A Acronyms and Definitions** ..... 16

**Attachment 1 DoD Information Systems User Agreement** ..... 26

**Attachment 2 DIL Software Protection Measures**..... 29

**Attachment 3 DIL Support Request Form** ..... 30

**UNCLASSIFIED**

***DIL***

17 May 2012

**LIST OF APPENDIXES**

STOCII-14-KOP-003

Enc 9-DIL SOP-4.0

---

**APPENDIX A - Acronyms and Definitions**

**LIST OF ATTACHMENTS**

**ATTACHMENT 1** – DoD Information System User Agreement

**ATTACHMENT 2** – DIL Software Protection Measures

**ATTACHMENT 3** – DIL Support Request Form

17 May 2012

---

**1.0 References**

- 1.0.1 DoD Directive 5220.20-M National Industrial Security Program Operating Manual (NISPOM)
- 1.0.2 PEO STRI JDIF Security Standard Operating Procedures
- 1.0.3 Central Technical Support Facility Army Interoperability Program Standard Operating Procedures

**1.1 Physical Security**

The physical security of the PEO STRI JDIF is the primary responsibility of PEO STRI. All personnel working within the PEO STRI DIL are responsible for maintaining the physical security, to include ensuring that all data (documents and media) complies with requirements for marking and labeling by clearly reflecting the appropriate classification or sensitivity level as required by DoD 5200-1R as well as ensuring that information regarding the DIL IS architecture is protected and not released to unauthorized personnel.

**1.2 Procedures For Sending Visit Access Request (VAR) To PEO STRI Joint Development Integration Facility (JDIF)**

Personnel with a valid need / requirement to visit the PEO STRI JDIF, Research Park, Orlando, Florida, must submit a visit request at least one week prior to the first day of the proposed visit in accordance with the guidelines provided below to ensure authorized access to the facilities. Please note that "Hand Carried" Visit Authorization Letters/Clearance Information will NOT be accepted. Access / Visit requests should be submitted via the JPAS system.

1. Visitors requiring unescorted access to the PEO STRI JDIF must have at a minimum of an Interim SECRET security clearance.
2. Visitors should plan to be signed into the facility prior to 1600 for badging.
3. Security managers must submit visit requests via JPAS to SMO Code W6ECA10.

Request must provide the following information:

- a. Social Security Number
- b. Clearance Level / Type Investigation / Investigation Date
- c. Purpose of Visit
- d. Date(s) of proposed visit (Provide justification for one-year certs)
- e. Place of Birth / Date of Birth / Citizenship
- f. Unit / Organization or Company
- g. Security Manager's Name, Signature & Date (person verifying clearance(s))
- h. Security Manager's Email or Phone#

Note: All visits will be verified via JPAS, must have "US Access" (Collateral / Non-SCI access) displayed or the visit request will "Not" be processed.

17 May 2012

PEO STRI Security Manager is: Stanley Slupski, [Stanley.Slupski@us.army.mil](mailto:Stanley.Slupski@us.army.mil)

Phone: (407) 384-5586.

**Facility Address**

PEO STRI JDIF  
12000 Research Parkway, Suite 300  
Orlando, FL 32826

To confirm receipt and approval of all visit request please call 407-384-3991.

**1.3 Procedures for non-permanent visitors granted JDIF access**

JDIF Unescorted Access Briefing

PEO STRI JDIF Security Awareness Briefing

NAVAIR Badge Application

- “Neither” box checked
- Items 33,34,36 checked
- Security Officer signs where indicated + by 24/7 + by each item
- Applicant signs on the back
- Security Officer makes a copy for security files and gives original to applicant
- Applicant takes the form to NAVAIR Pass & ID office

**1.4 JDIF SECRET Lab Uncleared Visitor Policy**

This policy governs visits to the DIL SECRET Lab when a visitor does not have an Interim SECRET or higher clearance on file with the JDIF. Though this policy provides guidance for bringing uncleared visitors in the SECRET Lab, it is not an endorsement of this practice.

The lab’s ability to support classified processing is part of what makes the lab valuable to the tenants. Bringing uncleared visitors into the SECRET Lab disrupts classified processing when it is taking place. Frequent disruptions devalue the lab because they prevent the lab from supporting classified processing. Therefore, everyone should consider the impact and weigh the benefit with the goal of keeping lab disruptions to a minimum.

**Policy**

- 1) All uncleared visits to the SECRET lab must be coordinated before hand with an authorized member of each program that leases space in the SECRET lab. Exceptions for

17 May 2012

prior coordination will be made for emergencies (e.g. equipment failure, hazardous condition, etc.).

NOTE: An uncleared visitor is someone who does not have verified collateral clearance information on file at the PEO STRI JDIF.

- 2) Tenant coordination must be conducted with someone who is authorized to grant or deny permission to suspend classified processing for a particular program. If you are unsure who is an authorized person, check with JDIF Security.
- 3) Once the proper coordination has been completed, red flashing lights turned on to alert everyone that an uncleared visitor is entering the lab.
- 4) An uncleared visitor must be escorted at all times. Only those persons who have received escort training are allowed to escort an uncleared visitor in the PEO STRI JDIF Lab area.
- 5) When the PEO STRI JDIF Lab is under sanitized condition (the flashing lights are on) ALL classified processing must be suspended until the lab is no longer under sanitized condition (the lights are off). Note: The lab remains under sanitized condition as long as the flashing lights are on – even if the uncleared visitor has left the lab.
- 6) When the PEO STRI JDIF Lab is under sanitized condition the ENTIRE lab is under sanitized condition. *"Adequate precautions must be taken to ensure that the uncleared and escorted visitor is prevented from viewing all systems and applications at all times"*.

**JDIF Security Violation Policy****Definition**

A security violation is the failure to comply with security requirements that could potentially result in the loss or compromise of classified information or an action that could cause harm to the United States of America. Below are some examples of security violations.

- Providing or facilitating access to classified information without first establishing a legitimate need to know.
- Allowing unauthorized or unsupervised personnel in a restricted area.
- Failing to notify all personnel before bringing uncleared person into a restricted area. Notification includes turning on warning lights.
- Failing to discontinue classified processing after consenting or acknowledging that uncleared person(s) is entering restricted area.
- Improperly handling or storing classified material.
- Removing classified data or material, including hardware devices, from a restricted area.  
**Note:** Security must be notified before removing any hardware device, including unclassified devices.
- Illegally or improperly accessing an information system.
- Illegally or improperly removing data from an information system.
- Bringing unauthorized equipment, including laptop computers, into the lab.
- Bringing unauthorized media into the lab. (**Note:** Approval of media into the lab does not mean that the media is authorized to be loaded on a system. You must contact the Program's System Administrator or Configuration Manager before loading software on any system within the JDIF.)
- Loading unauthorized software on an information system.
- Attempting to circumvent the security features of an information system.
- Intentionally introducing malicious code to an information system.

**Reporting**

Individuals that notice or discover any of the above violations must immediately report the incident to JDIF Security. If you become aware of a security violation and do not report it, you may be considered an accomplice and become subject to disciplinary action.

If you discover violation involving a suspected compromise to an information system, immediately contain the incident by unplugging the network cable. However, DO NOT do anything further to the system such as logging out, rebooting, or turning the system off. Performing any of these actions could destroy evidence and further compromise security.

**Disciplinary Action**

The Department of Defense Directive 5220.20-M, National Industrial Security Program Operating Manual (NISPOM), prescribes enforcement of a graduated scale of disciplinary action against employees who violate or show negligence toward security requirements. In the event an employee is found culpable of a security violation or negligence, the following disciplinary policy applies.

**First Offense** – JDIF Security will issue a Letter of Caution with a copy provided to the employee's Contract Program Manager. This letter will explain the seriousness of the violation as well as emphasize steps to prevent reoccurrence. The Letter of Caution will be placed in the employee's local security file but will not be sent to their Corporate Security Officer. The employee will be placed on probation for a period of twelve months. If there are no further violations during the probationary period, the Letter of Caution will be removed from the employee's security file and destroyed.

**Second Offense** – If a second offense occurs within the twelve-month probationary period described above, JDIF Security will issue a Letter of Reprimand with a copy provided to the Contract Program Manager and the Government Program Manager. The Letter of Reprimand will contain a warning of possible future disciplinary actions, as well as a notification to the Program Manager describing the corrective action to be implemented. This letter will be sent to the employee's Corporate Security Officer. The employee will be required to attend a full-scale security re-briefing.

**Third Offense** – If a third incident occurs within twenty-four months of the initial incident, JDIF Security will issue a Letter of Suspension with a copy provided to the employee's Contract Program Manager, Government Program Manager, and Corporate Security Officer. The Letter of Suspension will indefinitely withdraw access to classified information in the JDIF facility. A Disciplinary Review Panel comprised of JDIF Security and the Program Manager will convene a hearing to determine if and when access to classified information can be reinstated.

**NOTE:** All Security violations that are deemed serious enough or result from intentional circumvention of security requirements will be treated as a third offense. In all cases where violations of security policies and procedures occurred, JDIF Security will determine if the violation should be reported to the PEO STRI Security Office upon determination of the seriousness and nature of the violation.

## **1.5 Shipping Classified Material**

### Wrapping:

Classified material is double wrapped with opaque inner and outer wrappers.

### Inner wrapper:

- Envelopes are marked with appropriate classification on top and bottom of both sides.
- Boxes are marked with appropriate classification level on all surfaces
- Complete mailing address, to include the name of the cleared recipient, and complete return address

### Outer wrapper:

- Include complete mailing address and return address
- Address to Commander or other title, not an individual.
- No indication of classification

### Receipt:

- Fill in, print and sign FormCD-76F
- Attach receipt to inner envelope

Take package to receptionist.

### Shipper provides to receptionist:

- Ship to address
- Ship to phone number
- Weight of box
- Dimensions of box

Receptionist prepares FEDEX shipping label using JDIF on-line account (information in locked bottom drawer at reception desk) and provides Airbill number to shipper via email. Classified packages can only be shipped Priority Overnight, Monday through Thursday.

Shipper secures label to his package.

Receptionist schedules a pick up via telephone (1-800-463-3339) for same day pick up. Package is never left unattended in the reception lobby while waiting for FEDEX to arrive for pick up.

PEO STRI DIL support personnel and DIL customers will clear all classified material to be shipped from the facility through the facility security POC.

**Note: NEVER ship overnight on a Friday unless you have confirmed appropriate cleared personnel will be available to accept delivery on Saturday!!**

## **1.6 JDIF Opening / Closing Security Check**

For detailed instructions for Opening/Closing of the JDIF Lab please see or contact Stan Slupski, PEO STRI JDIF Security Manager.

## **2.0 COMPUTER AND NETWORK SECURITY PROCEDURES**

### **2.1 DoD Information System (IS) User Agreement**

All personnel that have been granted access to the JDIF Lab and prior to using DIL IS, will read this DIL SOP and sign a copy of the DoD Information System User Agreement, which will be kept on file for the duration of the simulation year. See Attachment 1 for a copy of the DoD Information System User Agreement Form.

### **2.2 Incoming Media and IS**

Media and/or IS must be brought to one of the DIL lab personnel to be scanned for viruses prior to entering the DIL. Upon a clean scan, the scanned items will be marked, dated and initialed.

CDs, DVDs, external hard drives and/or computer equipment are allowed for use in the JDIF and DIL facilities. The use of Thumb drives, flash or USB drives is expressly prohibited and Will Not be permitted.

### **2.3 Outgoing Media and IS**

When removing data and/or equipment from the DIL the item(s) must be brought to one of the DIL lab personnel to be properly processed out. The classification of all items intended for removal from the facility will be verified and all classified material will be cleared by the JDIF Security POC prior to removal.

## 2.4 Information Assurance Vulnerability Management (IAVM)

This SOP is based on the Joint Task Force-Global Network Operations (JTF-GNO) Information Assurance Vulnerability Management (IAVM) Program. The IAVM program is governed by DOD Directive CJCSM 6510.01 Change 2, dated 26 Jan 2006. The IAVM program focuses on managing the status of DOD networks to mitigate or eliminate known vulnerabilities. The IAVM program process includes three types of vulnerability notifications.

- a. **Information Assurance Vulnerability Alert (IAVA)**. An IAVA addresses severe network vulnerabilities resulting in immediate and potentially severe threats to DOD assets and information. Corrective action is of the highest priority due to the severity of the vulnerability risk.
- b. **Information Assurance Vulnerability Bulletin (IAVB)**. An IAVB addresses new vulnerabilities that do not pose an immediate risk to DOD assets, but are significant enough that noncompliance with the corrective action could escalate the risk.
- c. **Technical Advisory (TA)**. A TA addresses vulnerabilities that are generally categorized as low risk to DOD Assets.

### 2.4.1 IAVM Applicability and Scope

The IAVM program applies to any asset on any DOD owned, controlled, or contracted information system or network, to include (but not limited to) workstations, servers, routing and switching devices, firewalls, networked peripherals, and controlled interfaces (guards). An asset is considered a node on a network if it has its own network identification internet protocol (IP) address or media access control (MAC) address. **The applicability and scope apply even if the network or asset is in a test lab environment or in standalone mode (i.e. not connected to an external network)**. As such, this SOP uniformly applies to all DIL networks and standalone systems.

The primary DIL lab IAVM POC is Don Eady, DIL Lab Manager. The alternate is Dwayne Hoffman.

Each IAVM POC also should self subscribe to the IAVM notification lists. There is a subscription list for IAVAs, IAVBs, and TAs. As a subscriber, the IAVM POC will receive IAVAs, IAVBs, and TAs via email. The IAVM notice will contain information regarding the vulnerability and due dates for acknowledgment, first report, and plan of action/mitigation.

This SOP applies to only the DIL managed and controlled networks though the IAVM Program applies to all JDIF tenants.

**2.4.2 DIL Quarterly IAVA Updates**

The DIL as a recognized extension of the Central Technical Support Facility (CTSF) at Fort Hood, Texas receives and implements quarterly IAVA updates from the CTSF Configuration Management Office (CMO).

**2.4.3 Procedures for Applying Patches**

Upon receipt, the DIL applies the associated IAVA patches as directed and otherwise prescribed by the cognizant CTSF Information Security Official. The primary DIL IAVA POC or his designated alternate will ensure that the applicable patch (s) is installed on all effected DIL systems as directed. During the conduct of formal Army Interoperability Certification, IAVM updates will be applied to the portion of the DIL baseline architecture that is under CTSF CM Lockdown upon receipt of formal direction from the designated CTSF Test Officer in operational control of the on-going certification. Should the application of the IAVA patches not be allowed by the Test Officer during formal certification, they will be applied immediately upon release from CTSF CM Lockdown.

**3.0 DIL ARMY MISSION COMMAND (MC) SYSTEM INTEGRATION SUPPORT**

The DIL is a government owned, government operated, and contractor staffed facility for the purpose of supporting PEO STRI Programs and other DoD sponsored development, integration, test and certification activities. Accordingly, DIL support will only be afforded to those DoD sponsored activities with a valid DoD requirement and need to know.

**3.1 DIL Support Request Form (Appendix B)**

The DIL Support Request Form is used to facilitate the initial coordination for First Line MC system technical, integration, certification, test, validation and verification support resources. Requests are normally approved for a period of 90 days, however extensions will be granted on a as needed basis.

**3.2 Request for Loan of MC System Hardware (HW) and Software (SW)**

Request for loan of MC system HW, SW and other DIL Network Devices will be honored IAW the availability of DIL resources and de-conflicting previously approved support requests.

**4.0 FORMAL ARMY INTEROPERABILITY CERTIFICATION (AIC) SUPPORT**

During the conduct of formal AIC the DIL designated test architecture is under the operational control of the CTSF Test Directorate and designated CTSF Test Officer.

**4.1 Responsibilities of the System Under Test (SUT)**

It remains the responsibility of the Program Manager for the SUT or his/her designated representative to ensure compliance with all processes, policies, and procedures that govern the conduct of formal AIC (e.g. AIC Entrance and Exit Criteria).

DIL CTSF based personnel will support and otherwise assist with the coordination of and participation in AIC Certification Readiness Reviews (CRR), IPRs, and other meetings as requested by the cognizant program manager or designated representative. However, all decision authority rests with the responsible program manager or program representative.

**4.2 DIL Software Baseline and Network Architecture**

As an extension of the CTSF, the DIL SW Baseline, Army C4ISR and Simulation Initialization System (ACSIS) Data Products, and Network Architecture will be maintained IAW the prevailing CTSF Test Architecture.

**5.0 DIL MISSION COMMAND SYSTEM INTEGRATION SUPPORT**

To maximize the efficiencies gained by having a centralized integration facility, it is preferred that DIL integration support occur in the PEO STRI DIL facility. Support requests that require the displacement of DIL resources require prior coordination (DIL Support Form) and approval (Preferably one month prior). The DIL will endeavor to satisfy all request IAW the availability of resources and in consideration of previously scheduled support events that may occur concurrently.

**5.1 Pre-Event Meeting**

Pre-event meetings will be coordinated by the senior DIL System Engineer and the designated technical lead for the supported event. The intent is to conduct detailed planning and coordination required to ensure the best courses of action for a successful event.

**5.2 Post Event Meeting (AAR)**

Post event meetings are conducted to review the activities that occurred during the supported event in an effort to capture lessons learned and incorporate them into DIL processes, policies and procedures to facilitate DIL process improvement.

**5.3 Stand-alone Integration**

IAW paragraph 2.2, all incoming media and IS will be scanned by DIL personnel prior to being brought into the DIL. It is the responsibility of the supported activity to ensure that all incoming media and IS is IAVA compliant.

17 May 2012

When practical, DIL customers whose event objectives only require a subset of the DIL architecture the activity will be conducted in a stand-alone mode. It is the responsibility of the supported activity to define the support objectives and required support architecture needed to satisfy their respective requirement. Upon completion of the event, customer media and IS will be cleared to be removed from the DIL IAW paragraph 2.3.

All supporting DIL IS, media, and network devices will be scanned and returned to the overall DIL architecture.

## **6.0 FIREWALL AND INTRUSION DETECTION SYSTEM (IDS)**

The CISCO ASA 5510 Adaptive Security Appliance with AIP-SSM-10 is the implemented Firewall and Intrusion Detection System for the purpose of protecting and detecting unwanted attempts at accessing, manipulating, and/or disabling of the DIL Network or interconnecting systems.

**APPENDIX A****ACRONYMS AND DEFINITIONS**

**Access** - The ability and opportunity to obtain knowledge of classified information.

**Approved Security Container** - A security container for which the DSS has granted approval to store classified information.

**Audit Trails** - Audit trails provide a chronological record of IS usage and system support activities related to classified processing. They provide records of significant events occurring in the IS in sufficient detail to facilitate reconstruction, review, and examination of events involving possible compromise of classified information.

**Authentication** - The technique used to match the individual logging on to the IS with the user account being accessed. Examples of authentication techniques include, but are not limited to the following: passwords, tokens, biometrics, and smart cards.

**Authorized Persons** - Those persons who have a Need-To-Know (NTK) for the classified information in the performance of official duties (classified contact performance) and have been cleared for receipt of such information. When applicable, authorization will require a special briefing prior to receipt. Responsibility for determining whether duties require a person to possess or have access to any classified information and whether that person is authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipient.

**Authorized User** - Any individual with the written authorization and means to directly interact with the IS during a classified processing period. All users must have access authorization for all information contained in the IS during the classified processing period at Protection Level 1.

**CD-ROM** - Compact Disk - Read-Only Memory. A compact disk, which is closed and cannot be written with classified information.

**CD-RW** - Compact Disk - Read Write - A compact disk which maybe written with classified information or which is closed and cannot be written with any information.

**Certification** - The comprehensive evaluation of technical and non-technical security features to establish the extent to which an IS has met the security requirements necessary for it to process classified information. Certification precedes the accreditation. The certification is based upon an inspection and test to verify that the SSP accurately describes the IS configuration and

17 May 2012

operation.

**Classified Processing** - Entry, alteration, or removal of classified information or media on an IS. **Classified Processing Period**- The period from the initial entry of classified information or media into the IS until the completion of termination (downgrade and/or sanitization and declassification) procedures.

**Clearing** - Replacing the information in memory or on magnetic media with unclassified data. This procedure is used to initialize memory or media assuring no malicious or unauthorized code or software remains available. Clearing does not necessarily sanitize memory or media, but may be used to change the need-to-know associated with the memory of media.

**Closed Area** - A controlled area, as approved by the DSS, for the purpose of safeguarding classified material, which, because of its size and nature or operational necessity, cannot be adequately protected by the normal safeguards or stored during non-working hours in an approved security container. With explicit DSS approval a Closed Area maybe used for open storage of printed classified materials.

**Configuration Management (CM)**. A system of procedures describing the documentation, control, change, and maintenance of accountability of IS hardware, firmware, software, communications interfaces, operating procedures, and installation structures.

**Cognizant Security Agency** - The office responsible for IS accreditation, security administration, and compliance monitoring over a given classified activity, for all ISs compliant with the Master SSP, the Defense Security Service.

**Computer System** - An unaccredited system including computer hardware, software, and people to process data into useful information.

**COMSEC** - Communications Security. The protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures to electrical systems generating, handling, processing, or using National Security information and also includes the application of physical security measures to COMSEC information or materials.

**COMSEC Equipment** - Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment is CRYPTO equipment, crypto ancillary equipment, crypto production equipment, and authentication equipment. An example is a Network Encryption System (NES).

**COMSEC Material** - COMSEC aids, equipments, and components thereof, and devices that are identifiable by the telecommunications security (TSEC) nomenclature system or a similar system of a U.S. department or agency, foreign government, or international organization.

**Contract Security Classification Specification (DD Form 254)** - The form used by contracting activities to indicate security classification assigned to various elements of contracts. This form is the basic document, which identifies the specific items of information involved in a contract that requires security classification protection. Additionally, it provides the general administrative and contractual information pertaining to the security requirements of the classified effort. It may be supplemented with a Security Classification Guide (SCG).

**CPU** - Central Processing Unit.

**CRT**- Cathode Ray Tube.

**CRYPTO** - A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying National Security-related information. This CRYPTO marking also identifies COMSEC equipment and computer software containing operational keying variables.

**CSA** - Cognizant Security Agency. The Defense Security Service (DSS) is the CSA for all ISs compliant with the Master SSP.

**Data** - Any recorded information, regardless of its physical form or characteristics, exclusive of machinery, apparatus, equipment, or other items of material. The term includes, but is not limited to, the following: all written material, whether handwritten, printed, or typed; all photographs, negatives, exposed, or printed films, and still or motion pictures; all data processing cards or tapes; charts; paintings; drawings; engravings; sketches; working notes and papers; and all reproduction of the foregoing for whatever process reproduced; and sound voice, video, or electronic recordings in any form. (The term "data" is synonymous with the term "document.")

**DD 254** - Department of Defense Form 254, Department of Defense Contract Security Classification Specification. This form is the basic document, which identifies the specific items of information involved in a contract that requires security classification protection. Additionally, it provides the general administrative and contractual information pertaining to the security requirements of the classified effort. It may be supplemented with a Security Classification Guide\ (SCG).

**Declassification\ (IS)** - Following sanitization, an administrative determination that classified information has been totally eradicated from a storage media or memory. Components are declassified in only two situations: (1) the component is being removed from safeguards to be repaired OR (2) the component will no longer be used for classified processing.

**Degauss** - To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process.

**Degausser** - An electrical device or hand-held permanent magnet assembly that generates a coercive magnetic force for degaussing magnetic storage media.

**Designated Accrediting Authority (DAA)** - The customer, User Agency, or other Government organization who has the authority to decide on accepting the security safeguards prescribed. Reviews and accredits the SSP and grants accreditation to process classified information on an IS. The Designated Accrediting Authority for contracts to comply with this document is the Defense Security Service (DSS).

**DoD** - Department of Defense.

**Downgrade (IS)** - To adjust the IS to a lower security level for: processing a lower level or less restrictive type of classified information, changing from a classified to an unclassified processing period, or establishing a level of continuous physical protection when the IS is not to be used.

**DRAM** - Dynamic Random Access Memory.

**DSS** - Defense Security Service.

**DVD-ROM** - Digital Versatile Disk - Read only media A Digital versatile media disk, which is closed and cannot be written with classified information.

**DVD-RW** - Digital Versatile Disk - Read Write - A digital versatile disk which maybe written with classified information or which is closed and cannot be written with any information.

**EAPROM** - Electronically Alterable Programmable Read-Only Memory.

**EEPROM** - Electronically Erasable Programmable Read-Only Memory.

**EPOM** - Erasable Programmable Read-Only Memory.

**Facility** - A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which related by function or location, form an operating entity. A business or educational organization may consist of one or more facilities. For purposes of industrial security, this term does not include Government installations.

**FEPROM** - Flash Erasable Programmable Read-Only Memory.

**Firmware** - A method of organizing control or an IS in a microprogrammed structure in addition to, or rather than, software or hardware. Microprograms are composed of microinstructions, normally implemented in read-only memory, to control the sequencing of computer circuits directly at the detailed level of the single machine instruction. Firmware is addressed as hardware memory at P&W.

**FSO** - Facility Security Officer. This is the manager of security operations at each facility.

**GCA** - Government Contracting Agency.

**IAM** - Information Assurance Manager. This is an employee appointed by the Facility Security Officer and responsible for the implementation and administration of IS Security Policy, operational compliance, and maintenance with the documented security measures and controls, and ensure an on going IS security education program at the contractor facility.

**IAO** - Information Assurance Officer. This is the individual responsible for monitoring the IS on a continuing basis. The IAO ensures the hardware, software, installation, and maintenance, as applicable, conform to appropriate requirements and monitors access to each assigned IS. Note: formerly called an IS Custodian.

**IDS** - Intrusion Detection System.

**Information Processing Equipment** - Any equipment or device that electromechanically or electronically processes, reproduces, converts, or otherwise manipulates any form of information. The following equipment is typical: electrical typewriters; reproduction copies; word processors; digital photography equipment; composing and editing equipment; video displays; automated data processors; telecommunications equipment and systems including teletype, facsimile, and

17 May 2012

cryptographic equipment; and all interfaces, modems, and interconnecting paths that are part of the system or equipment.

**Information Security** - The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information the protection of which is authorized by Executive Order of statute.

**Information System (IS)** - An accredited assembly of computer hardware, software, firmware, facilities, personnel and procedures configured for the purpose of automating the functions of computing, sequencing, storing, retrieving, displaying, communications, or otherwise manipulating data, information, and textual material. In the context of this document, an IS includes any and all components which are accredited to contain or process classified information and any and all components which are connected.

**Interconnected Network** - Separately accredited ISs and/or unified networks in which each self-contained IS maintains its own intra-IS services and controls, protects its own resources, retains its individual accreditation, and each participating IS or unified network has its own ISSM

**IS Hardware** - Any physical equipment or device used in the configuration and operation of an IS, includes general-purpose and special-purpose digital, analog, and hybrid computers that perform logical, arithmetic, or storage functions; and all components directly related to or operating in conjunction with such computers that are used to create, compose, collect, store, edit, process, communicate, display, or disseminate information.

**IS Security** - The totality of security safeguards needed to provide an acceptable level of protection for an IS and the classified data processed. Includes all hardware and software functions, characteristics, and mechanisms; operational accountability and access control procedures at the computer and remote terminal facilities and management constraints; physical structures and devices needed to provide an acceptable level of protection for classified information in any state of storage, processing, display or communication; and fire control systems, flight navigation, or simulations stored or displayed or communicated within the IS.

**JDIF** – Joint Digital Integration Facility

**LAN** - Local Area Network.

**Magnetic Media** - Any material having the capability to store information in a magnetic form. This includes tapes, floppy disks, hard disks, and magnetic cards.

**MC** – Mission Command.

**MOU** - Memorandum of Understanding. Formal agreement of understanding between connected

17 May 2012

facilities defining the security procedures for the network used for classified processing between two or more CSAs. An MOU is not required for STU-III or STE connections.

**NES** - Network Encryption System. A secure communications platform incorporating communications security standards and INFOSEC (Information Security) design principles to protect classified information on LANs (Local Area Networks), interconnected LANs, and Wide Area Networks (WANs) by National Security Agency) authorized Type 1 encryption.

**Network** - A computing environment with more than one independent processor interconnected to permit communications and sharing of resources. See also Interconnected Network and Unified Network.

**NISP** - National Industrial Security Program.

**NISPOM** - National Industrial Security Program Operating Manual (DoD5220.22-M).

**Non-Standalone IS** - An IS which does not conform to the restrictions of a standalone IS (reference Standalone IS).

**Non-Volatile Memory** - Memory that does not lose its capacity to retain data when power is removed.

**NVRAM** - Nonvolatile Random Access Memory. A type of volatile memory made nonvolatile by using batteries or capacitors to provide power and retain information when power is switched off.

**NSA** - National Security Agency.

**NSM** - Network Security Manager.

**NTK** - Need-To-Know. A determination made by the processor of classified information that a prospective recipient, in the interest of National Security, has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or Program approved by a User Agency.

**Operating System** - An integrated collection of computer programs that controls all resources of an IS, internally manages job flow through the computer, and plays a central role in ensuring the secure operation of the IS.

**PEO STRI** – Program Executive Office for Simulation, Training, and Instrumentation.

**Protection Profile** - An IS security procedure document used to define a particular IS protection environment and referenced to the Master SSP.

**PCL** - Personnel Clearance Level. A determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel security clearance being granted.

**Periods Processing** - A mode where an IS, which is authorized to process classified information related to multiple Programs, is dedicated in each period to only one Program and/or has downgraded periods for unclassified processing.

**Personal Computing System** - Any electronic device with memory which may store or process information. May be a single unit or a collection of interconnected devices, which are controlled by a single individual. Includes, but is not limited to, programmable calculators, memory typewriters, standalone word processors, and personal computers (PCs). Excludes devices, which support multiple terminals/workstations when performing classified work.

**PIN** - Personal Identification Number.

**Privileged User** - An individual who has authorization and access to change the configuration of the IS and administer the accounts and access of other users. This includes an individual who makes changes to security-relevant software.

**PROM** - Programmable Read-Only Memory.

**RAM** - Random-Access Memory. A standard type of volatile memory used in computing and test equipment. May be battery- or capacitor-backed to retain information when power is switched off making it NVRAM.

**ROM** - Read-Only Memory.

**Sanitization** - The technical eradication of classified data from magnetic media. This action is followed by the administrative declassification of the media when applicable.

**SCSI** - Small Computer System Interface. A standard used to connect devices to small computers like workstations and PCs. The SCSI controller on some hard disks prevents the identification of bad blocks (defects) and, thus, these disks cannot be sanitized, but must be destroyed to declassify them.

**Security-Relevant Software** - IS operating system, access control, virus detection, and sanitization programs used while processing classified information and accredited on the Protection Profile Software Baseline.

**Security Classification Guide (SCG)** - A document issued by an authorized original classifier which prescribes the level of classification and appropriate declassification instructions for specific information to be classified on a derivative basis. SCGs are provided to contractors as a supplement to the Contract Security Classification Specification (DD254).

**Security Clearance** - A determination that a facility or individual is eligible for access to classified information of the same or lower category as the clearance granted; synonymous with PCL.

**Security Container** - A container such as a file cabinet whose modifications have been approved by the DSS for the storage of classified information. May also include containers made, procured, and approved by the General Services Administration (GSA).

**SIPRNET** - SECRET Internet Protocol Router Network - A DoD network for classified connection of contractors to Government facilities. This network is managed by DISA (Defense Information Systems Agency).

**Software** - Computer programs, procedures, rules, information, databases, and data concerned with and needed for the operation of an IS.

**Special Briefings** - The special briefings relevant to IS security are the following: COMSEC (Communication Security), NATO (North Atlantic Treaty Organization), SAP (Special Access Program), and SCI (Sensitive Compartmented Information).

**SRAM** - Static Random Access Memory.

**SSP** - System Security Plan - Documentation required to obtain approval and accreditation for a classified IS. Unless otherwise stated, the SSP shall refer to the Master SSP and the appropriate Protection Profile.

**Standalone IS** - An IS which has the following restrictions while operating in classified mode: a single user interface, no network or remote communications, no software disconnects employed for disabling unapproved devices, and all equipment under the immediate control of the IS user.

**SUT** - System Under Test

**TEMPEST** - An unclassified short name referring to investigations and study of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals which, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled or otherwise processed by any information processing equipment. EMSEC (Emanation Security) is also used to refer to this aspect of IS security.

17 May 2012

---

**Transmission** - The sending of information from one location to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for classified material from one authorized addressee to another.

**TVAR** - TEMPEST Vulnerability Assessment Request. Documentation concerning IS processing and its vulnerability to interception of compromising emanations.

**Unauthorized Person** - Any person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

**Unified Network** - A collection of ISs or network systems, which are accredited as a single entity by a single CSA usually with one SSP.

**Upgrade (IS)** - To adjust the IS to a higher security level for initiating a classified processing period after the IS has not been in use, changing from an unclassified to a classified processing period, or processing a higher level or more restrictive type of classified information.

**User Agencies** - Those U.S. Government departments or agencies identified as having ownership of or cognizance over specific classified information.

**Users** - Any person who interacts directly with an IS or networked system.

**VAL** - Visit Authorization Letter.

**Virus** - Malicious software; a form of Trojan horse reproducing itself in other executable code.

**Volatile Memory** - Memory that loses its capacity to retain data when power is removed.

**WAN** - Wide Area Network. This generally connects geographically remote sites.

**Workstation** - A high performance, microprocessor-based computing platform using specialized software applicable to the work environment.

**WORM** - Write Once, Read Many media

## Attachment 1 – DoD Information System User Agreement and Acceptable Use Policy

### DIL INTEGRATION LAB DoD INFORMATION SYSTEMS USER AGREEMENT & ACCEPTABLE USE POLICY

DIL Lab Personnel                       PEO STRI                       Visitor/Company:

---

PRINT NAME

PHONE

Per DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems-Standard Consent Banner and User Agreement," May 9, 2008, I understand that the DIL Integration Lab is a DoD Secret, restricted area, and that I must be in possession of a secret clearance before accessing the premises. I further understand that as an automated information system (AIS) user, it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification or destruction of information. I have read the DIL Standard Operation Procedure (SOP) for the DIL LAB to which I have access and agree to comply with the terms/restrictions as listed below:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government use only.
- You consent to the following conditions:
  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and s data stored on this information system.
  - Communications using, or data store on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.
  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user’s consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

**UNCLASSIFIED**

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or a data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
- o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- o All of the above conditions apply regardless of whether the access or used of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

• **Minimum security rules and requirements:** As an XXXXX user, the following security rules and requirements apply:

- a. I will not be permitted access to the DIL unless I am in complete compliance with the JDIF personnel security requirements for operating in a classified environment, and possess a need-to-know.
- b. I have completed the user security awareness-training module. I will participate in all required training program before receiving access privileges to the system.
- c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 14 characters with two (2) each of uppercase and lowercase letters, numbers, and special characters. I am

**UNCLASSIFIED**

- the only authorized user of this account. I will not use my User ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.
- d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, or public domain software (i.e. USB drives, freeware, or shareware).
  - e. I will use virus-checking procedures before uploading or accessing information from any subsystem, diskette, attachment, memory stick, or compact disk.
  - f. I will not attempt to access or process data exceeding the authorized classification level of the DIL, which is classified SECRET or below, in nature.
  - g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.
  - h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code and introduce it into the subsystem.
  - i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the DIL and will not disseminate it to anyone without a specific need-to-know.
  - j. I will not utilize Army or DOD provided information systems for commercial financial gain or illegal activities.
  - k. Only the System Administrator (SA) or Department of Defense authorized personnel will perform hardware and software maintenance.
  - l. I will use screen locks and log off the workstation (portable or fixed) when departing the operational area.
  - m. I will immediately report any suspicious output, files, shortcuts, or system problems to the JDIF FSO, PM CONSIM IAM, and DIL IASO and cease all activities on the subsystem.
  - n. I will be familiar with the DIL Incident Response Plan.
  - o. I will address any questions regarding policy, responsibilities, and duties to the DIL SA or IASO.
  - p. I understand that the DIL is the property of the Army and is provided to me for official and authorized uses. I further understand that the DIL information system is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the DIL and may have only a limited expectation of privacy in personal data on the DIL. I realize that I should not store data on the DIL that I do not want others to see or use.
  - q. I understand that monitoring of the DIL will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. **I understand that the following activities define unacceptable uses of an Army information system:**
    - Use for personal commercial gain or illegal activities.
    - Use in any manner that interferes with official duties or violates standards of ethical conduct.
    - Send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (e.g., spam) communications. (Law enforcement investigators or attorneys operating in their official capacities are exempt from this requirement.)
    - Participate in on-line gambling or other activities inconsistent with public service.
    - Participate in, install, configure, or use IS's in any commercial or personal Distributed Computing Environment (DCE) (e.g., SETI, human genome research).
    - Release, disclose, or alter any sensitive, proprietary, or classified information without the consent of the data owner, the Original Classification Authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.
    - Forward or auto-forward official mail to non-official accounts or devices.

**UNCLASSIFIED**

- Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring; except for privileged users and authorized uses.
  - Modify or use the system equipment or software in any manner other than its intended purpose.
  - Introduce malicious software or code, e.g., Trojan horses, Worms, Viruses, Trap Doors, or Back Doors.
  - Relocate or change equipment or the network connectivity of equipment without supervisor authorization.
  - Share personal accounts and passwords.
  - Permit the use of remote access capabilities by any unauthorized individual.
  - Disable or remove security or protective software or mechanisms and their associated logs.
  - Place any classified data on any file system.
- r. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information requested below could result in denial of access to the DIL.

**ACKNOWLEDGMENT OF BRIEFING**

I have read and understand the above terms/restrictions. I understand that if my User ID or I is suspect of misuse or abuse of the DIL Integration Facility automated information systems and resources, that investigation and disciplinary action may be taken. If I am the laboratory director, group supervisor, systems administrator, or IAO, I will ensure that all users in my area of responsibility sign this agreement.

---

SIGNATURE

DATE

## Attachment 2 – DIL Software Protection Measures

### PROTECTION MEASURES:

- a. Use of the PEO STRI DIL Mission Command (MC) application software shall be limited to use by DIL Customers IAW the PEO STRI Material Fielding Exception Licensing Agreement. The DIL MC software is not for commercial use.
- b. The DIL MC software shall not be provided, even temporarily, to anyone outside of the Recipient's management control; issuance to contractor personnel is only permitted in accordance with paragraph c, below.
- c. The Recipient agrees that DIL software will not be released to any commercial company that is not in direct and/or developmental support (via contract) of the DoD user's intent for the software.
- d. The DIL MC software shall only be installed on Government owned computers under the control of the signature authority and their organization. The total number of copies installed shall not exceed the number of licensed and authorized copies and released by the applicable PM.
- e. The Recipient agrees to use the DIL MC system(s) only in a manner that does not violate the terms and conditions of the individual software licenses. Recipients shall adhere to the specific software terms & conditions and software license requirements as well as any other conditions associated with the software provided, and manage authorizations regarding seat allocations, annual licensing renewals, upgrade and/or update entitlements, agreement expiration dates, authorized copies, authorized users, etc as applicable.
- f. The Recipient agrees to not modify or make copies of the DIL MC software nor to give it to any other unit or organization without prior written coordination and approval of the DIL.
- g. The Recipient agrees to return all DIL software (media) on loan or in temporary use, to the DIL upon completion of the project or upon request by a DIL representative.
- h. The Recipient agrees that DIL MC software will not be demonstrated to any commercial company that is not in direct and/or developmental support (via contract) of the software, or to personnel that do not have a "need to know" and/or the appropriate clearances without prior coordination through the DIL.

