Security Control Mapping

1. Background

The Department of the Navy (DON) uses Information Systems (IS) and Information Technology (IT) to leverage the power of information through sharing and collaborating securely. The DON uses the Certification and Accreditation (C&A) process to assess and understand the residual risk associated with operating IS and IT.

Because the need to share information securely has grown beyond individual communities and spread across the entire Federal government and beyond, it became imperative that we change our approach to C&A in order to meet these needs.

As a result, the DON is participating with the Department of Defense (DoD) the Intelligence Community (IC), and the rest of the Federal government in C&A transformation. Through C&A transformation, the DON will strengthen its ability to deploy more rapidly IS and IT, enabling information sharing securely between and with others.

One goal of C&A transformation is to achieve common security controls enabling the DON, the DoD, the IC, and the rest of the federal government to develop systems to the same protection standards, which the deploying community would apply appropriately for the security level of the IS or IT. In doing so, and along with other goals and initiatives, facilitates reciprocity of approvals and reuse of systems across communities.

The goal to achieve common security controls further specified using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as the base document for common security controls. Recently, NIST published SP 800-53, revision 3, which is the consolidated catalog of security controls.

The DON will continue to use the DoDI 8500.2 as the authoritative source for security controls until otherwise specified. However, knowing and understanding the changes represented in NIST SP 800-53r3, will be essential once the DON begins to transition to this new set of security controls. For that reason, the DON CIO developed security control mappings using the NIST SP 800-53r3 and existing DoD and IC security control documents.

2. Purpose

Mappings between the security controls delineated within NIST SP 800-53r3 and those listed in DoDI 8500.2 will be useful in support of updating and modifying the certification documentation associated with systems certified and accredited under the existing C&A standards. Accordingly, the appendices of this document contain such mappings.

3. Descriptions

a. Appendix A – DoDI 8500.2 Security Control Mapping

This table maps each DoDI 8500.2 security control to the related NIST SP 800-53r3 security control(s). The NIST SP 800-53 to DoDI 8500.2 security control mappings from Appendix G of

NIST SP 800-53r2 was used as the initial foundation for this table. Those associations were individually validated against NIST SP 800-53r3 and new associations were added, as appropriate, for new or modified security controls and each control enhancement in NIST SP 800-53r3. The information in each column of the table is described below.

(1) The first column lists all of the DoDI 8500.2 security controls in alphabetic order.

(2) The second column lists the DoDI 8500.2 control name.

(3) The next three columns indicate, as appropriate, Mission Assurance Category(ies) to which the control is associated as well as to which IA Service the control is related, either Integrity (I) or Availability (A).

(4) The sixth through eighth columns indicates, as appropriate, which confidentiality level(s) the control is associated with as well as which IA Service the control is related to, either Confidentiality (C), Integrity (I), or Availability (A).

(5) The ninth column lists the related NIST SP 800-53r3 security control or control enhancement number.

(6) The tenth column lists the control name associated with the NIST SP 800-53r3 security control number in the ninth column.

(7) The eleventh through thirteen columns indicates the applicable security control baseline(s) of the NIST SP 800-53r3 security control or control enhancement.

(8) The final 12 columns (14 through 25) display the CNSSI 1253 primary control objectives (C, I, &/or A) and baseline impact level(s) (Low (L), Moderate (M), &/or High (H)) related to the NIST SP 800-53r3 security control or control enhancement (listed in columns ten and eleven). This portion of the table was extracted directly from Tables D-1 and D-2 of CNSSI 1253. Appendix D of CNSSI 1253 should be consulted for further information about how this *binning* was established.

b. **Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with MAC Level I. The column descriptions in this table are the same as in Appendix A, as provided above.

c. **Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with MAC Level II. The column descriptions in this table are the same as in Appendix A, as provided above.

d. **Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with MAC Level III. The column descriptions in this table are the same as in Appendix A, as provided above.

e. **Appendix E – DoDI 8500.2 Security Control Mapping for Systems Processing Classified Information**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with systems processing classified information. The column descriptions in this table are the same as in Appendix A, as provided above.

f. **Appendix F – DoDI 8500.2 Security Control Mapping for Systems Processing Sensitive Information**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with systems processing Sensitive information. The column descriptions in this table are the same as in Appendix A, as provided above.

g. **Appendix G – DoDI 8500.2 Security Control Mapping for Systems Processing Public Information**

This table is a filtered listing of only those DoDI 8500.2 controls, listed in Appendix A, that are associated with systems processing Public information. The column descriptions in this table are the same as in Appendix A, as provided above.

h. **Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls**

This table is a listing of the NIST SP 800-53r3 security controls that have no associations to any of the security controls contained in DoDI 8500.2. The column descriptions in this table are the same as in Appendix A, as provided above.

i. **Appendix I – NIST SP 800-53r3 Security Control Mapping**

This table is a reverse of mapping to that of Appendices A through H. It maps each individual NIST SP 800-53r3 security control and control enhancement to the related DoDI 8500.2 security control(s). Additionally it provides a similar mapping to the related DCID 6/3 security control(s) (The NIST SP 800-53 to DCID 6/3 security control mappings from Appendix G of NIST SP 800-53r2 was used for this portion of the table; modified or additional mappings for revision 3 of NIST SP 800-53 have yet to be generated.). Most of the column descriptions in this table are similar to those in Appendix A, as provided above, but they now appear in a different order. Those reordered column descriptions are reiterated below for clarity, as well including descriptions for the new columns associated with the DCID 6/3 mapping.

(1) The first column lists the NIST SP 800-53r3 controls and control enhancements in alphabetic and numeric order.

(2) The second column lists the NIST SP 800-53r3 control name.

*[Note: Those controls and enhancements listed in **blue** font are new additions to the third revision of NIST SP 800-53. This table also shows where control names where changed from the second revision of the document, and likewise shows where controls and enhancements were deleted or otherwise combined with other controls as part of the revision process.]*

(3) The next three columns indicate the applicable security control baseline(s) of the NIST SP 800-53r3 security control.

(4) The sixth column lists the related DoDI 8500.2 security control number(s).

*[Note: As discussed above for Appendix A, the NIST SP 800-53 to DoDI 8500.2 security control mappings from Appendix G of NIST SP 800-53r2 was used as the initial foundation for the indicated mapping. Those associations were individually validated against NIST SP 800-53r3 and new associations were added, as appropriate, for the new or modified security controls and for each control enhancement in NIST SP 800-53r3. The resulting new association additions are indicated in **green** font in this table.]*

(5) The seventh through ninth columns indicates Mission Assurance Category(ies) to which the DoDI 8500.2 control is associated as well as to which IA Service the control is related, either Integrity (I) or Availability (A).

(6) The tenth through twelfth columns indicates which confidentiality level(s) the DoDI 8500.2 control is associated with as well as which IA Service the control is related to, either Confidentiality (C), Integrity (I), or Availability (A).

(7) Similar to the sixth column, the thirteenth column lists the DCID 6/3 security control(s) related to the NIST SP 800-53r3 control.

(8) The fourteenth column indicates, if appropriate, the Confidentiality Protection Level for the DCID 6/3 control.

(9) The fifteenth and sixteenth columns indicate, if appropriate, the Integrity and Availability Level of Confidence for the DCID 6/3 control.

(10) Similar to Appendix A, the final 12 columns (17 through 28) display the CNSSI 1253 primary control objectives (C, I, &/or A) and baseline impact level(s) (Low (L), Moderate (M), &/or High (H)) related to the NIST SP 800-53r3 security control or control enhancement (listed in columns ten and eleven).

4. **Discussion**

The appendices in this document can be used to aid in the re-certification of systems transitioning from a DoDI 8500.2 security control baseline to a NIST SP 800-53v3 or CNSSI

1253 security control baseline. Appendices A through G will assist with determining which NIST SP 800-53r3 controls are associated with the DoDI 8500.2 controls that may already be addressed in the certification documentation and system design.

Appendix H of this document may be useful in a different manner. It will assist with identifying which additional NIST SP 800-53v3 security controls, with no association to the DoDI 8500.2 controls, may not have been addressed under the legacy DoDI 8500.2 security control baselines of prior certifications. These additional controls may drive system modifications or configuration changes, and/or additions or changes to system operations or security management.

Appendix I of this document should help in understanding how the security controls for a system categorized using the NIST or CNSSI guidelines would map to the legacy security controls of DoDI 8500.2. This might assist in determining how a security control was previously addressed or if the control is new, with no association to a DoDI 8500.2 categorization and underlying security control.

While this document is focused primarily on transitioning from DoDI 8500.2 to NIST SP 800-53r3 and CNSSI 1253, it is anticipated that a similar analysis, mapping and set of tables might prove equally useful for the transition from DCID 6/3 and the JDCSISSS to NIST SP 800-53r3 and CNSSI 1253.

5. Point of Contact

Please address all questions, comments or recommendations regarding this document, the inclusive tables, or the security control mappings to:

“Ask an Expert” on the DON CIO web site
http://www.doncio.navy.mil/AskAnExpert.aspx

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
COAS-1	Alternate Site Designation			A				CP-7	Alternate Processing Site		X	X									X		X	X
COAS-2	Alternate Site Designation	A	A					CP-7	Alternate Processing Site		X	X									X		X	X
		A	A					CP-7(4)	Alternate Processing Site (Control Enhancement)			X									X		X	X
COBR-1	Protection of Backup and Restoration Assets	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-6	Alternate Storage Site		X	X									X		X	X
CODB-1	Data Backup Procedures			A				CP-9	Information System Backup	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CODB-2	Data Backup Procedures		A					CP-6	Alternate Storage Site		X	X									X		X	X
			A					CP-9	Information System Backup	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CODB-3	Data Backup Procedures	A						CP-9(6)	Information System Backup (Control Enhancement)												X			
CODP-1	Disaster and Recovery Planning			A				CP-2(3)	Contingency Plan (Control Enhancement)			X									X			X
CODP-2	Disaster and Recovery Planning		A					CP-2(4)	Contingency Plan (Control Enhancement)												X			X
CODP-3	Disaster and Recovery Planning	A						CP-2(5)	Contingency Plan (Control Enhancement)												X			X
COEB-1	Enclave Boundary Defense			A				CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X			X	X			X	X	X		X	X
				A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
COEB-2	Enclave Boundary Defense	A	A					CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X			X	X			X	X	X		X	X
		A	A					SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
COED-1	Scheduled Exercises and Drills		A	A				CP-4	Contingency Plan Testing and Exercises	X	X	X									X	X	X	X
COED-2	Scheduled Exercises and Drills	A						CP-4	Contingency Plan Testing and Exercises	X	X	X									X	X	X	X
COEF-1	Identification of Essential Functions			A				CP-2	Contingency Plan	X	X	X									X	X	X	X
COEF-2	Identification of Essential Functions	A	A					CP-2	Contingency Plan	X	X	X									X	X	X	X
COMS-1	Maintenance Support			A				MA-6	Timely Maintenance		X	X									X		X	X
COMS-2	Maintenance Support	A	A					MA-6	Timely Maintenance		X	X									X		X	X
COPS-1	Power Supply			A				PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
				A				PE-11(2)	Emergency Power (Control Enhancement)												X			X
COPS-2	Power Supply		A					PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
			A					PE-11(2)	Emergency Power (Control Enhancement)												X			X
COPS-3	Power Supply	A						PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
		A						PE-11(2)	Emergency Power (Control Enhancement)												X			X
COSP-1	Spares and Parts		A	A				CP-7	Alternate Processing Site		X	X									X		X	X
			A	A				MA-6	Timely Maintenance		X	X									X		X	X
COSP-2	Spares and Parts	A						CP-7	Alternate Processing Site		X	X									X		X	X
		A						MA-6	Timely Maintenance		X	X									X		X	X
COSW-1	Backup Copies of Critical SW	A	A	A				CP-9(3)	Information System Backup (Control Enhancement)			X									X			X
COTR-1	Trusted Recovery	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
DCAR-1	Procedural Review	A	A	A				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		A	A	A				CA-2(1)	Security Assessments (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
		A	A	A				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-1	System and Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCAS-1	Acquisition Standards				C	C	C	SA-4(6)	Acquisitions (Control Enhancement)								X		X	X				
					C	C	C	SA-4(7)	Acquisitions (Control Enhancement)								X		X	X				
DCBP-1	Best Security Practices	I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SA-8	Security Engineering Principles		X	X					X		X	X				
DCCB-1	Control Board			I				CM-3	Configuration Change Control		X	X					X		X	X				
DCCB-2	Control Board	I	I					CM-3	Configuration Change Control		X	X					X		X	X				
		I	I					CM-3(4)	Configuration Change Control (Control Enhancement)								X		X	X				
DCCS-1	Configuration Specifications			I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
				I				SA-8	Security Engineering Principles		X	X					X		X	X				
DCCS-2	Configuration Specifications	I	I					CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I					SA-8	Security Engineering Principles		X	X					X		X	X				
DCCT-1	Compliance Testing	I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				CM-4(2)	Security Impact Analysis (Control Enhancement)								X							
		I	I	I				CM-6(4)	Configuration Settings (Control Enhancement)								X							
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCDS-1	Dedicated IA Services	I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
		I	I	I				SA-9(1)	External Information System Services (Control Enhancement)								X		X	X				
DCFA-1	Functional Architecture for AIS Applications	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				PL-2(1)	System Security Plan (Control Enhancement)				X		X	X	X		X	X	X		X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I	I				PM-7	Enterprise Architecture	X	X	X	X				X				X			
		I	I	I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCHW-1	HW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCID-1	Interconnection Documentation	I	I	I				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-5(2)	Information System Documentation (Control Enhancement)			X					X			X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCII-1	IA Impact Assessment	I	I	I				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-3(2)	Configuration Change Control (Control Enhancement)		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCIT-1	IA for IT Services	I	I	I				PS-7	Third-Party Personnel Security	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCMC-1	Mobile Code	I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SC-18	Mobile Code		X	X					X	X	X	X				
DCNR-1	Non-repudiation	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				AU-10(5)	Non-repudiation (Control Enhancement)								X		X	X				
DCPA-1	Partitioning the Application	I	I	I				SC-2	Application Partitioning		X	X	X		X	X	X		X	X				
DCPB-1	IA Program and Budget	A	A					SA-2	Allocation of Resources	X	X	X					X	X	X	X				
DCPD-1	Public Domain Software Controls	A	A	A				SA-6	Software Usage Restrictions	X	X	X	X	X	X	X	X	X	X	X				
DCPP-1	Ports, Protocols, and Services	A	A	A				CM-7(1)	Least Functionality (Control Enhancement)		X	X	X		X	X	X		X	X				
		A	A	A				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCPR-1	CM Process	I	I	I				CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				CM-3	Configuration Change Control		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I	I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I	I				CM-9	Configuration Management Plan		X	X					X		X	X				
DCSD-1	IA Documentation	A	A	A				PL-2	System Security Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCSL-1	System Library Management Controls	I	I	I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
DCSP-1	Security Support Structure Partitioning	I	I					SC-3	Security Function Isolation			X	X		X	X	X		X	X				
DCSQ-1	Software Quality	I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				SA-11(1)	Developer Security Testing (Control Enhancement)								X							
		I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCSR-1	Specified Robustness - Basic						C	SA-4	Acquisitions	X	X	X					X	X	X	X				
DCSR-2	Specified Robustness - Medium					C		SA-4	Acquisitions	X	X	X					X	X	X	X				
DCSR-3	Specified Robustness – High				C			SA-4	Acquisitions	X	X	X					X	X	X	X				
DCSS-1	System State Changes			I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
				I				SI-6	Security Functionality Verification			X					X		X	X				
DCSS-2	System State Changes	I	I		I			SI-6	Security Functionality Verification			X					X		X	X				
DCSW-1	SW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
EBBD-1	Boundary Defense						C	AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
							C	CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
							C	CA-3(1)	Information System Connections (Control Enhancement)				X											
EBBD-1	Boundary Defense						C	SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
							C	SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBBD-2	Boundary Defense					C		AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
						C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
						C		CA-3(1)	Information System Connections (Control Enhancement)				X											
						C		SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
						C		SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBBD-3	Boundary Defense				C			AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
					C			CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
					C			CA-3(2)	Information System Connections (Control Enhancement)				X	X	X	X								
					C			SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
					C			SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBCR-1	Connection Rules	A	A	A				AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
		A	A	A				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBPW-1	Public WAN Connection					C	C	CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
						C	C	SC-14	Public Access Protections	X	X	X					X	X	X	X	X	X	X	X
						C	C	SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBRP-1	Remote Access for Privileged Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(7)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
					C	C		MA-4	Non-Local Maintenance	X	X	X					X	X	X	X				
					C	C		MA-4(1)	Non-Local Maintenance (Control Enhancement)		X	X					X		X	X				
					C	C		MA-4(6)	Non-Local Maintenance (Control Enhancement)				X				X							
EBRU-1	Remote Access for User Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253														
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
					C	C		IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-17	Alternate Work Site		X	X	X		X	X	X		X	X	X		X	X
					C	C		SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBVC-1	VPN Controls	A	A	A				SI-4(10)	Information System Monitoring Tools and Techniques (Control Enhancement)				X		X	X	X		X	X				
ECAD-1	Affiliation Display				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
ECAN-1	Access for Need-to-Know				C	C		AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		AC-2(6)	Account Management (Control Enhancement)				X				X							
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(3)	Access Enforcement (Control Enhancement)				X				X							
					C	C		AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECAR-1	Audit Record Content – Public Systems						C	AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
							C	AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
							C	AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAR-2	Audit Record Content – Sensitive Systems					C		AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
						C		AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
						C		AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAR-3	Audit Record Content – Classified Systems Audit of Security Label Changes				C			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			I		I	I	AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	I	I		I			AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-5	Response to Audit Processing Failures	X	X	X									X	X	X	X
		I	I		I			AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			IR-4(5)	Incident Handling (Control Enhancement)				X				X							
ECCD-1	Changes to Data			I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
ECCD-2	Changes to Data	I	I		I			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECCM-1	COMSEC				C			SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			SC-8	Transmission Integrity		X	X					X	X	X	X				
					C			SC-9	Transmission Confidentiality		X	X	X	X	X	X								
ECCR-1	Encryption for Confidentiality (Data at Rest)					C		MP-4	Media Storage		X	X	X	X	X	X								
						C		SC-13(1)	Use of Cryptography (Control Enhancement)				X											
						C		SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
ECCR-2	Encryption for Confidentiality (Data at Rest)				C			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C			MP-4	Media Storage		X	X	X	X	X	X								
					C			SC-13(3)	Use of Cryptography (Control Enhancement)				X											
					C			SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				
ECCR-3	Encryption for Confidentiality (Data at Rest)				C			MP-4	Media Storage		X	X	X	X	X	X								
					C			SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								
					C			SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				
ECCT-1	Encryption for Confidentiality (Data at Transmit)					C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
						C		AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X				
						C		SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECCT-2	Encryption for Confidentiality (Data at Transmit)				C			SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECDC-1	Data Change Controls	I	I					CP-10(2)	Information System Recovery and Reconstitution (Control Enhancement)		X	X					X		X	X	X		X	X
ECIC-1	Interconnections among DoD Systems and Enclaves				C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(4)	Access Enforcement (Control Enhancement)				X	X	X	X	X	X	X	X				
					C	C		AC-4(14)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		AC-4(15)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
ECID-1	Host Based IDS	I	I					SC-7(12)	Boundary Protection (Control Enhancement)				X		X	X	X		X	X			X	X
		I	I					SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
ECIM-1	Instant Messaging	I	I	I				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		I	I	I				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SC-15(2)	Collaborative Computing Devices (Control Enhancement)				X		X	X	X		X	X				
		I	I	I				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECLC-1	Audit Record Content – Classified Systems Audit of Security Label Changes				C			AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-8	Time Stamps	X	X	X					X	X	X	X				
ECLO-1	Logon					C		AC-10	Concurrent Session Control			X					X		X	X				
						C		AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	X	X		X	X	X
ECLO-2	Logon				C			AC-10	Concurrent Session Control			X					X		X	X				
					C			AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	X	X		X	X	X
					C			AC-9	Previous Logon (Access) Notification								X		X	X				
ECLP-1	Least Privilege				C	C	C	AC-5	Separation of Duties		X	X	X		X	X	X		X	X				
					C	C	C	AC-6	Least Privilege		X	X	X		X	X	X		X	X				
ECML-1	Marking and Labeling				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
					C	C		MP-3	Media Marking		X	X	X	X	X	X								
ECMT-1	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECMT-2	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253														
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECND-1	Network Device Controls			I				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
				I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
ECND-2	Network Device Controls	I	I					AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
		I	I					CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X				
ECNK-1	Encryption for Need-To-Know				C	C		SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECNK-2	Encryption for Need-To-Know				C			SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECPA-1	Privileged Account Control	I	I	I				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AC-2(7)	Account Management (Control Enhancement)				X		X	X	X		X	X				
ECPC-1	Production Code Change Controls			I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
ECPC-2	Production Code Change Controls	I	I					CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
ECRC-1	Resource Control				C	C		SC-4	Information In Shared Resources		X	X	X		X	X								
ECRG-1	Audit Reduction and Report Generation	I	I	I				AU-7	Audit Reduction and Report Generation		X	X	X		X	X	X		X	X				
ECRR-1	Audit Record Retention				I	I	I	AU-11	Audit Record Retention	X	X	X									X	X	X	X
ECSC-1	Security Configuration Compliance	A	A	A				CM-6	Configuration Settings	X	X	X					X	X	X	X				
ECSD-1	Software Development Change Controls			I				CM-5	Access Restrictions for Change		X	X					X		X	X				
ECSD-2	Software Development Change Controls	I	I					CM-3	Configuration Change Control		X	X					X		X	X				
		I	I					CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X				
		I	I					AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
ECTB-1	Audit Trail Backup	I	I	I				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AU-9(2)	Protection of Audit Information (Control Enhancement)												X			
ECTC-1	Tempest Controls				C	C		AC-18(5)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
					C	C		PE-19	Information Leakage				X		X	X			X	X				
ECTM-1	Transmission Integrity Controls			I				SC-8	Transmission Integrity		X	X					X	X	X	X				
				I				SI-7	Software and Information Integrity		X	X					X		X	X				
ECTM-2	Transmission Integrity Controls	I	I					SC-16	Transmission of Security Attributes				X		X	X	X		X	X				
		I	I					SC-8	Transmission Integrity		X	X					X	X	X	X				
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X				
ECTP-1	Audit Trail Protection		I	I				AU-9	Protection of Audit Information	X	X	X	X	X	X	X	X	X	X	X				
ECVI-1	Voice-over-IP (VoIP) Protection	A	A	A				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-15	Collaborative Computing Devices	X	X	X	X	X	X	X								
		A	A	A				SC-19	Voice Over Internet Protocol		X	X	X		X	X	X		X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECVP-1	Virus Protection	A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
ECWM-1	Warning Message				C	C	C	AC-8	System Use Notification	X	X	X	X	X	X	X	X	X	X	X				
ECWN-1	Wireless Computing and Network	A	A	A				AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				AC-19	Access Control for Mobile Devices	X	X	X	X	X	X	X	X	X	X	X				
IAAC-1	Account Control				C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
					C	C		PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
IAGA-1	Group Authentication				C	C		IA-2(5)	User Identification and Authentication (Organizational Users) (Control Enhancement)				X		X	X	X		X	X				
					C	C		IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
					C	C		IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
IAIA-1	Individual Identification and Authentication					C		IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-5(1)	Authenticator Management (Control Enhancement)	X	X	X	X		X	X	X		X	X				
						C		IA-5(3)	Authenticator Management (Control Enhancement)								X		X	X				
						C		IA-5(5)	Authenticator Management (Control Enhancement)				X				X							
						C		IA-5(6)	Authenticator Management (Control Enhancement)				X	X	X	X	X	X	X	X				
IAIA-2	Individual Identification and Authentication				C			IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-5(1)	Authenticator Management (Control Enhancement)	X	X	X	X		X	X	X		X	X				
					C			IA-5(3)	Authenticator Management (Control Enhancement)								X		X	X				
					C			IA-5(5)	Authenticator Management (Control Enhancement)				X				X							
					C			IA-5(6)	Authenticator Management (Control Enhancement)				X	X	X	X	X	X	X	X				
IAKM-1	Key Management			I				IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12(2)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-12(4)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-13(1)	Use of Cryptography (Control Enhancement)				X											
				I				SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
IAKM-2	Key Management	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-13(1)	Use of Cryptography (Control Enhancement)				X											
		I	I					SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I					SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
IAKM-3	Key Management				I			IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
					I			SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								
					I			SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
IATS-1	Token and Certificate Standards			I				IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12(4)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
IATS-2	Token and Certificate Standards	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
PECF-1	Access to Computing Facilities					C		PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PECF-2	Access to Computing Facilities				C			PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-2(3)	Physical Access Authorizations (Control Enhancement)				X	X	X	X								
PECS-1	Clearing and Sanitizing					C		MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
						C		MP-6(4)	Media Sanitization (Control Enhancement)				X											
PECS-2	Clearing and Sanitizing				C			MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
					C			MP-6(5)	Media Sanitization (Control Enhancement)				X	X	X	X								
PEDD-1	Destruction				C			MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
					C			MP-6(6)	Media Sanitization (Control Enhancement)				X	X	X	X								
PEDI-1	Data Interception				I	I		MP-2	Media Access	X	X	X	X	X	X	X								
					I	I		PE-5	Access Control for Output Devices		X	X	X		X	X								
PEEL-1	Emergency Lighting			A				PE-12	Emergency Lighting	X	X	X									X	X	X	X
PEEL-2	Emergency Lighting	A	A					PE-12	Emergency Lighting	X	X	X									X	X	X	X
		A	A					PE-12(1)	Emergency Lighting (Control Enhancement)												X		X	X
PEFD-1	Fire Detection			A				PE-13	Fire Protection	X	X	X									X	X	X	X
PEFD-2	Fire Detection	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A					PE-13(1)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X
PEFI-1	Fire Inspection	A	A	A				PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A	A				PE-13(4)	Fire Protection (Control Enhancement)												X		X	X
PEFS-1	Fire Suppression			A				PE-13	Fire Protection	X	X	X									X	X	X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253												
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
PEFS-2	Fire Suppression	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(3)	Fire Protection (Control Enhancement)		X	X									X		X	X
PEHC-1	Humidity Controls			A				PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
				A				PE-14(2)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PEHC-2	Humidity Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PEMS-1	Master Power Switch	A	A	A				PE-10	Emergency Shutoff		X	X									X		X	X
PEPF-1	Physical Protection of Facilities					C		MP-2	Media Access	X	X	X	X	X	X	X								
						C		PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		PE-5	Access Control for Output Devices		X	X	X		X	X								
PEPF-2	Physical Protection of Facilities				C			MP-2	Media Access	X	X	X	X	X	X	X								
					C			PE-2(2)	Physical Access Authorizations (Control Enhancement)				X				X							
					C			PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-3(3)	Physical Access Control (Control Enhancement)				X	X	X	X	X	X	X	X				
					C			PE-5	Access Control for Output Devices		X	X	X		X	X								
					C			PE-6	Monitoring Physical Access	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-6(1)	Monitoring Physical Access (Control Enhancement)		X	X									X		X	X
					C			PE-8	Access Records	X	X	X	X	X	X	X	X	X	X	X				
PEPS-1	Physical Security Testing				C	C		CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
					C	C		PE-3(6)	Physical Access Control (Control Enhancement)								X			X				
PESL-1	Screen Lock	I	I	I				AC-11	Session Lock		X	X	X	X	X	X	X	X	X	X				
		I	I	I				AC-11(1)	Session Lock (Control Enhancement)				X	X	X	X								
PESP-1	Workplace Security Procedures				C	C		MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		SI-12	Information Output Handling and Retention	X	X	X	X	X	X	X	X	X	X	X				
PESS-1	Storage				C	C		MP-4	Media Storage		X	X	X	X	X	X								
PETC-1	Temperature Controls			A				PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
				A				PE-14(2)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PETC-2	Temperature Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PETN-1	Environmental Control Training	A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PEVC-1	Visitor Control to Computing Facilities				C	C		PE-7	Visitor Control	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-8	Access Records	X	X	X	X	X	X	X	X	X	X	X				
PEVR-1	Voltage Regulators	A	A	A				PE-9(2)	Power Equipment and Power Cabling (Control Enhancement)												X		X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253														
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
PRAS-1	Access to Information					C		AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		PS-3	Personnel Screening	X	X	X	X	X	X	X	X	X	X	X				
						C		PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
						C		PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
PRAS-2	Access to Information				C			AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PS-3	Personnel Screening	X	X	X	X	X	X	X	X	X	X	X				
					C			PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C			PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								
PRMP-1	Maintenance Personnel					C	C	MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C	C	MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PRMP-2	Maintenance Personnel				C			MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(1)	Maintenance Personnel (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(2)	Maintenance Personnel (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(3)	Maintenance Personnel (Control Enhancement)				X				X				X			
PRNK-1	Access to Need-to-Know Information				C	C	C	AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
					C	C	C	PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	A	A	A				PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PRTN-1	Information Assurance Training				I	I		AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-2	Security Awareness	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-3	Security Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		CP-3	Contingency Training	X	X	X									X	X	X	X
					I	I		IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIIR-1	Incident Response Planning		A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-3	Incident Response Testing and Exercises		X	X	X		X	X	X		X	X	X		X	X
			A	A				IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIIR-2	Incident Response Planning	A						IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-3	Incident Response Testing and Exercises		X	X	X		X	X	X		X	X	X		X	X
		A						IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix A – DoDI 8500.2 Security Control Mapping

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253												
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		A						IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIVM-1	Vulnerability Management	A	A	A				CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
		A	A	A				RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
		A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
		A	A	A				SI-5	Security Alerts, Advisories, and Directives	X	X	X					X	X	X	X				

Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I

DoDI 8500.2								NIST SP 800-53r3							CNSSI 1253											
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
COAS-2	Alternate Site Designation	A	A					CP-7	Alternate Processing Site		X	X									X		X	X
		A	A					CP-7(4)	Alternate Processing Site (Control Enhancement)			X									X		X	X
COBR-1	Protection of Backup and Restoration Assets	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-6	Alternate Storage Site		X	X									X		X	X
CODB-3	Data Backup Procedures	A						CP-9(6)	Information System Backup (Control Enhancement)												X			
CODP-3	Disaster and Recovery Planning	A						CP-2(5)	Contingency Plan (Control Enhancement)												X			X
COEB-2	Enclave Boundary Defense	A	A					CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X			X	X			X	X	X		X	X
		A	A					SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
COED-2	Scheduled Exercises and Drills	A						CP-4	Contingency Plan Testing and Exercises	X	X	X									X	X	X	X
COEF-2	Identification of Essential Functions	A	A					CP-2	Contingency Plan	X	X	X									X	X	X	X
COMS-2	Maintenance Support	A	A					MA-6	Timely Maintenance		X	X									X		X	X
COPS-3	Power Supply	A						PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
		A						PE-11(2)	Emergency Power (Control Enhancement)												X			X
COSP-2	Spares and Parts	A						CP-7	Alternate Processing Site		X	X									X		X	X
		A						MA-6	Timely Maintenance		X	X									X		X	X
COSW-1	Backup Copies of Critical SW	A	A	A				CP-9(3)	Information System Backup (Control Enhancement)			X									X			X
COTR-1	Trusted Recovery	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
DCAR-1	Procedural Review	A	A	A				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2(1)	Security Assessments (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
		A	A	A				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-1	System and Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCBP-1	Best Security Practices	I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SA-8	Security Engineering Principles		X	X					X		X	X				
DCCB-2	Control Board	I	I					CM-3	Configuration Change Control		X	X					X		X	X				

Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253														
		M	A	C		CN				BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I					CM-3(4)	Configuration Change Control (Control Enhancement)								X		X	X				
DCCS-2	Configuration Specifications	I	I					CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I					SA-8	Security Engineering Principles		X	X					X		X	X				
DCCT-1	Compliance Testing	I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				CM-4(2)	Security Impact Analysis (Control Enhancement)								X							
		I	I	I				CM-6(4)	Configuration Settings (Control Enhancement)								X							
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCDS-1	Dedicated IA Services	I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
		I	I	I				SA-9(1)	External Information System Services (Control Enhancement)								X		X	X				
DCFA-1	Functional Architecture for AIS Applications	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				PL-2(1)	System Security Plan (Control Enhancement)				X		X	X	X		X	X	X		X	X
		I	I	I				PM-7	Enterprise Architecture	X	X	X	X				X				X			
		I	I	I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCHW-1	HW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCID-1	Interconnection Documentation	I	I	I				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-5(2)	Information System Documentation (Control Enhancement)			X					X			X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCII-1	IA Impact Assessment	I	I	I				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-3(2)	Configuration Change Control (Control Enhancement)		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCIT-1	IA for IT Services	I	I	I				PS-7	Third-Party Personnel Security	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCMC-1	Mobile Code	I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SC-18	Mobile Code		X	X					X	X	X	X				
DCNR-1	Non-repudiation	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				AU-10(5)	Non-repudiation (Control Enhancement)								X		X	X				
DCPA-1	Partitioning the Application	I	I	I				SC-2	Application Partitioning		X	X	X		X	X	X		X	X				
DCPB-1	IA Program and Budget	A	A					SA-2	Allocation of Resources	X	X	X					X	X	X	X				
DCPD-1	Public Domain Software Controls	A	A	A				SA-6	Software Usage Restrictions	X	X	X	X	X	X	X	X	X	X	X				
DCPP-1	Ports, Protocols, and Services	A	A	A				CM-7(1)	Least Functionality (Control Enhancement)		X	X	X		X	X	X		X	X				
		A	A	A				SA-9	External Information System Services	X	X	X					X	X	X	X				

Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
DCPR-1	CM Process	I	I	I				CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				CM-3	Configuration Change Control		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I	I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I	I				CM-9	Configuration Management Plan		X	X					X		X	X				
DCSD-1	IA Documentation	A	A	A				PL-2	System Security Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCSL-1	System Library Management Controls	I	I	I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
DCSP-1	Security Support Structure Partitioning	I	I					SC-3	Security Function Isolation			X	X		X	X	X		X	X				
DCSQ-1	Software Quality	I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				SA-11(1)	Developer Security Testing (Control Enhancement)								X							
		I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCSS-2	System State Changes	I	I		I			SI-6	Security Functionality Verification			X					X		X	X				
DCSW-1	SW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
EBCR-1	Connection Rules	A	A	A				AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
		A	A	A				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBVC-1	VPN Controls	A	A	A				SI-4(10)	Information System Monitoring Tools and Techniques (Control Enhancement)				X		X	X	X		X	X				
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	I	I		I			AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-5	Response to Audit Processing Failures	X	X	X									X	X	X	X
		I	I		I			AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			IR-4(5)	Incident Handling (Control Enhancement)				X				X							
ECCD-2	Changes to Data	I	I		I			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECDC-1	Data Change Controls	I	I					CP-10(2)	Information System Recovery and Reconstitution (Control Enhancement)		X	X					X		X	X	X		X	X
ECID-1	Host Based IDS	I	I					SC-7(12)	Boundary Protection (Control Enhancement)				X		X	X	X		X	X			X	X
		I	I					SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
ECIM-1	Instant Messaging	I	I	I				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		I	I	I				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SC-15(2)	Collaborative Computing Devices (Control Enhancement)				X		X	X	X		X	X				
		I	I	I				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECND-2	Network Device Controls	I	I					AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
		I	I					CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X

Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X				
ECPA-1	Privileged Account Control	I	I	I				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AC-2(7)	Account Management (Control Enhancement)				X		X	X	X		X	X				
ECPC-2	Production Code Change Controls	I	I					CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
ECRG-1	Audit Reduction and Report Generation	I	I	I				AU-7	Audit Reduction and Report Generation		X	X	X		X	X	X		X	X				
ECSC-1	Security Configuration Compliance	A	A	A				CM-6	Configuration Settings	X	X	X					X	X	X	X				
ECSD-2	Software Development Change Controls	I	I					CM-3	Configuration Change Control		X	X					X		X	X				
		I	I					CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X				
		I	I					AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
ECTB-1	Audit Trail Backup	I	I	I				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AU-9(2)	Protection of Audit Information (Control Enhancement)												X			
ECTM-2	Transmission Integrity Controls	I	I					SC-16	Transmission of Security Attributes				X		X	X	X		X	X				
		I	I					SC-8	Transmission Integrity		X	X					X	X	X	X				
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X				
ECVI-1	Voice-over-IP (VoIP) Protection	A	A	A				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-15	Collaborative Computing Devices	X	X	X	X	X	X	X								
		A	A	A				SC-19	Voice Over Internet Protocol		X	X	X		X	X	X		X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECVP-1	Virus Protection	A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
ECWN-1	Wireless Computing and Network	A	A	A				AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				AC-19	Access Control for Mobile Devices	X	X	X	X	X	X	X	X	X	X	X				
IAKM-2	Key Management	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-13(1)	Use of Cryptography (Control Enhancement)				X											
		I	I					SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								
		I	I					SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
IATS-2	Token and Certificate Standards	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
PEEL-2	Emergency Lighting	A	A					PE-12	Emergency Lighting	X	X	X									X	X	X	X
		A	A					PE-12(1)	Emergency Lighting (Control Enhancement)												X		X	X
PEFD-2	Fire Detection	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A					PE-13(1)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X

Appendix B – DoDI 8500.2 Security Control Mapping for Mission Assurance Category I

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253											
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
PEFI-1	Fire Inspection	A	A	A				PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A	A				PE-13(4)	Fire Protection (Control Enhancement)												X		X	X
PEFS-2	Fire Suppression	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(3)	Fire Protection (Control Enhancement)		X	X									X		X	X
PEHC-2	Humidity Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PEMS-1	Master Power Switch	A	A	A				PE-10	Emergency Shutoff		X	X									X		X	X
PESL-1	Screen Lock	I	I	I				AC-11	Session Lock		X	X	X	X	X	X	X	X	X	X				
		I	I	I				AC-11(1)	Session Lock (Control Enhancement)				X	X	X	X								
PETC-2	Temperature Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PETN-1	Environmental Control Training	A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PEVR-1	Voltage Regulators	A	A	A				PE-9(2)	Power Equipment and Power Cabling (Control Enhancement)												X		X	X
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	A	A	A				PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIIR-2	Incident Response Planning	A						IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-3	Incident Response Testing and Exercises		X	X	X		X	X	X		X	X	X		X	X
		A						IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A						IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIVM-1	Vulnerability Management	A	A	A				CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
		A	A	A				RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
		A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
		A	A	A				SI-5	Security Alerts, Advisories, and Directives	X	X	X					X	X	X	X				

Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253											
		M	A	C	CN					BL				C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
COAS-2	Alternate Site Designation	A	A					CP-7	Alternate Processing Site		X	X									X		X	X
		A	A					CP-7(4)	Alternate Processing Site (Control Enhancement)			X									X		X	X
COBR-1	Protection of Backup and Restoration Assets	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-6	Alternate Storage Site		X	X									X		X	X
CODB-2	Data Backup Procedures		A					CP-6	Alternate Storage Site		X	X									X		X	X
			A					CP-9	Information System Backup	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CODP-2	Disaster and Recovery Planning		A					CP-2(4)	Contingency Plan (Control Enhancement)												X			X
COEB-2	Enclave Boundary Defense	A	A					CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X			X	X			X	X	X		X	X
		A	A					SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
COED-1	Scheduled Exercises and Drills		A	A				CP-4	Contingency Plan Testing and Exercises	X	X	X									X	X	X	X
COEF-2	Identification of Essential Functions	A	A					CP-2	Contingency Plan	X	X	X									X	X	X	X
COMS-2	Maintenance Support	A	A					MA-6	Timely Maintenance		X	X									X		X	X
COPS-2	Power Supply		A					PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
			A					PE-11(2)	Emergency Power (Control Enhancement)												X			X
COSP-1	Spares and Parts		A	A				CP-7	Alternate Processing Site		X	X									X		X	X
			A	A				MA-6	Timely Maintenance		X	X									X		X	X
COSW-1	Backup Copies of Critical SW	A	A	A				CP-9(3)	Information System Backup (Control Enhancement)			X									X			X
COTR-1	Trusted Recovery	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
DCAR-1	Procedural Review	A	A	A				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2(1)	Security Assessments (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
		A	A	A				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-1	System and Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCBP-1	Best Security Practices	I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SA-8	Security Engineering Principles		X	X					X		X	X				

Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II

DoDI 8500.2								NIST SP 800-53r3							CNSSI 1253											
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
DCCB-2	Control Board	I	I					CM-3	Configuration Change Control		X	X					X		X	X				
		I	I					CM-3(4)	Configuration Change Control (Control Enhancement)								X		X	X				
DCCS-2	Configuration Specifications	I	I					CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I					SA-8	Security Engineering Principles		X	X					X		X	X				
DCCT-1	Compliance Testing	I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				CM-4(2)	Security Impact Analysis (Control Enhancement)								X							
		I	I	I				CM-6(4)	Configuration Settings (Control Enhancement)								X							
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCDS-1	Dedicated IA Services	I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
		I	I	I				SA-9(1)	External Information System Services (Control Enhancement)								X		X	X				
DCFA-1	Functional Architecture for AIS Applications	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				PL-2(1)	System Security Plan (Control Enhancement)				X		X	X	X		X	X	X		X	X
		I	I	I				PM-7	Enterprise Architecture	X	X	X	X				X				X			
		I	I	I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCHW-1	HW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCID-1	Interconnection Documentation	I	I	I				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-5(2)	Information System Documentation (Control Enhancement)			X					X			X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCII-1	IA Impact Assessment	I	I	I				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-3(2)	Configuration Change Control (Control Enhancement)		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCIT-1	IA for IT Services	I	I	I				PS-7	Third-Party Personnel Security	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCMC-1	Mobile Code	I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SC-18	Mobile Code		X	X					X	X	X	X				
DCNR-1	Non-repudiation	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				AU-10(5)	Non-repudiation (Control Enhancement)								X		X	X				
DCPA-1	Partitioning the Application	I	I	I				SC-2	Application Partitioning		X	X	X		X	X	X		X	X				
DCPB-1	IA Program and Budget	A	A					SA-2	Allocation of Resources	X	X	X					X	X	X	X				
DCPD-1	Public Domain Software Controls	A	A	A				SA-6	Software Usage Restrictions	X	X	X	X	X	X	X	X	X	X	X				
DCPP-1	Ports, Protocols, and Services	A	A	A				CM-7(1)	Least Functionality (Control Enhancement)		X	X	X		X	X	X		X	X				

Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C		CN				BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		A	A	A				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCPR-1	CM Process	I	I	I				CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				CM-3	Configuration Change Control		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I	I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I	I				CM-9	Configuration Management Plan		X	X					X		X	X				
DCSD-1	IA Documentation	A	A	A				PL-2	System Security Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCSL-1	System Library Management Controls	I	I	I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
DCSP-1	Security Support Structure Partitioning	I	I					SC-3	Security Function Isolation			X	X		X	X	X		X	X				
DCSQ-1	Software Quality	I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				SA-11(1)	Developer Security Testing (Control Enhancement)								X							
		I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCSS-2	System State Changes	I	I		I			SI-6	Security Functionality Verification			X					X		X	X				
DCSW-1	SW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
EBCR-1	Connection Rules	A	A	A				AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
		A	A	A				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBVC-1	VPN Controls	A	A	A				SI-4(10)	Information System Monitoring Tools and Techniques (Control Enhancement)				X		X	X	X		X	X				
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	I	I		I			AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-5	Response to Audit Processing Failures	X	X	X									X	X	X	X
		I	I		I			AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			IR-4(5)	Incident Handling (Control Enhancement)				X				X							
ECCD-2	Changes to Data	I	I		I			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECDC-1	Data Change Controls	I	I					CP-10(2)	Information System Recovery and Reconstitution (Control Enhancement)		X	X					X		X	X	X		X	X
ECID-1	Host Based IDS	I	I					SC-7(12)	Boundary Protection (Control Enhancement)				X		X	X	X		X	X			X	X
		I	I					SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
ECIM-1	Instant Messaging	I	I	I				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		I	I	I				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SC-15(2)	Collaborative Computing Devices (Control Enhancement)				X		X	X	X		X	X				
		I	I	I				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECND-2	Network Device Controls	I	I					AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				

Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C		CN				BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I					CP-10	Information System Recovery and Reconstitution	X	X	X													X	X	X	X
		I	I					SA-5	Information System Documentation	X	X	X					X	X	X	X								
ECPA-1	Privileged Account Control	I	I	I				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AC-2(7)	Account Management (Control Enhancement)				X		X	X	X		X	X							
ECPC-2	Production Code Change Controls	I	I					CM-5(5)	Access Restrictions for Change (Control Enhancement)								X										
ECRG-1	Audit Reduction and Report Generation	I	I	I				AU-7	Audit Reduction and Report Generation		X	X	X		X	X	X		X	X							
ECSC-1	Security Configuration Compliance	A	A	A				CM-6	Configuration Settings	X	X	X					X	X	X	X							
ECSD-2	Software Development Change Controls	I	I					CM-3	Configuration Change Control		X	X					X		X	X							
		I	I					CM-5	Access Restrictions for Change		X	X					X		X	X							
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X							
		I	I					AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X							
ECTB-1	Audit Trail Backup	I	I	I				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AU-9(2)	Protection of Audit Information (Control Enhancement)												X						
ECTM-2	Transmission Integrity Controls	I	I					SC-16	Transmission of Security Attributes				X		X	X	X		X	X							
		I	I					SC-8	Transmission Integrity		X	X					X	X	X	X							
		I	I					SI-7	Software and Information Integrity		X	X					X		X	X							
ECTP-1	Audit Trail Protection		I	I				AU-9	Protection of Audit Information	X	X	X	X	X	X	X	X	X	X	X							
ECVI-1	Voice-over-IP (VoIP) Protection	A	A	A				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X							
		A	A	A				SC-15	Collaborative Computing Devices	X	X	X	X	X	X	X											
		A	A	A				SC-19	Voice Over Internet Protocol		X	X	X		X	X	X		X	X							
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X							
ECVP-1	Virus Protection	A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X							
ECWN-1	Wireless Computing and Network	A	A	A				AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X							
		A	A	A				AC-19	Access Control for Mobile Devices	X	X	X	X	X	X	X	X	X	X	X							
IAKM-2	Key Management	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X							
		I	I					SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X							
		I	I					SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X									
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X									
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X							
		I	I					SC-13(1)	Use of Cryptography (Control Enhancement)				X													
		I	I					SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X										
		I	I					SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X							
IATS-2	Token and Certificate Standards	I	I					IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X							
		I	I					SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X									
		I	I					SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X							
PEEL-2	Emergency Lighting	A	A					PE-12	Emergency Lighting	X	X	X									X	X	X	X			
		A	A					PE-12(1)	Emergency Lighting (Control Enhancement)												X		X	X			
PEFD-2	Fire Detection	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X			

Appendix C – DoDI 8500.2 Security Control Mapping for Mission Assurance Category II

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253												
		M	A	C	CN					BL			C				I				A				
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		A	A					PE-13(1)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X
PEFI-1	Fire Inspection	A	A	A				PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A	A				PE-13(4)	Fire Protection (Control Enhancement)												X		X	X
PEFS-2	Fire Suppression	A	A					PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A					PE-13(2)	Fire Protection (Control Enhancement)		X	X									X		X	X
		A	A					PE-13(3)	Fire Protection (Control Enhancement)		X	X									X		X	X
PEHC-2	Humidity Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PEMS-1	Master Power Switch	A	A	A				PE-10	Emergency Shutoff		X	X									X		X	X
PESL-1	Screen Lock	I	I	I				AC-11	Session Lock		X	X	X	X	X	X	X	X	X	X				
		I	I	I				AC-11(1)	Session Lock (Control Enhancement)				X	X	X	X								
PETC-2	Temperature Controls	A	A					PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
		A	A					PE-14(1)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PETN-1	Environmental Control Training	A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PEVR-1	Voltage Regulators	A	A	A				PE-9(2)	Power Equipment and Power Cabling (Control Enhancement)												X		X	X
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	A	A	A				PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIIR-1	Incident Response Planning		A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-3	Incident Response Testing and Exercises		X	X	X		X	X	X		X	X	X		X	X
			A	A				IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIVM-1	Vulnerability Management	A	A	A				CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
		A	A	A				RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
		A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
		A	A	A				SI-5	Security Alerts, Advisories, and Directives	X	X	X					X	X	X	X				

Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III

DoDI 8500.2								NIST SP 800-53r3							CNSSI 1253											
		M	A	C		CN				BL			C					I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL.	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
COAS-1	Alternate Site Designation			A				CP-7	Alternate Processing Site		X	X									X		X	X
COBR-1	Protection of Backup and Restoration Assets	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-6	Alternate Storage Site		X	X									X		X	X
CODB-1	Data Backup Procedures			A				CP-9	Information System Backup	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CODP-1	Disaster and Recovery Planning			A				CP-2(3)	Contingency Plan (Control Enhancement)			X									X			X
COEB-1	Enclave Boundary Defense			A				CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X			X	X			X	X	X		X	X
				A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
COED-1	Scheduled Exercises and Drills		A	A				CP-4	Contingency Plan Testing and Exercises	X	X	X									X	X	X	X
COEF-1	Identification of Essential Functions			A				CP-2	Contingency Plan	X	X	X									X	X	X	X
COMS-1	Maintenance Support			A				MA-6	Timely Maintenance		X	X									X		X	X
COPS-1	Power Supply			A				PE-11(1)	Emergency Power (Control Enhancement)			X									X		X	
				A				PE-11(2)	Emergency Power (Control Enhancement)												X			X
COSP-1	Spares and Parts		A	A				CP-7	Alternate Processing Site		X	X									X		X	X
			A	A				MA-6	Timely Maintenance		X	X									X		X	X
COSW-1	Backup Copies of Critical SW	A	A	A				CP-9(3)	Information System Backup (Control Enhancement)			X									X			X
COTR-1	Trusted Recovery	A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
DCAR-1	Procedural Review	A	A	A				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				CA-2(1)	Security Assessments (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
		A	A	A				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-1	System and Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCBP-1	Best Security Practices	I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SA-8	Security Engineering Principles		X	X					X		X	X				
DCCB-1	Control Board			I				CM-3	Configuration Change Control		X	X					X		X	X				
DCCS-1	Configuration Specifications			I				SA-5	Information System Documentation	X	X	X					X	X	X	X				

Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C		CN				BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL.	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
				I				SA-8	Security Engineering Principles		X	X					X		X	X				
DCCT-1	Compliance Testing	I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				CM-4(2)	Security Impact Analysis (Control Enhancement)								X							
		I	I	I				CM-6(4)	Configuration Settings (Control Enhancement)								X							
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCDS-1	Dedicated IA Services	I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
		I	I	I				SA-9(1)	External Information System Services (Control Enhancement)								X		X	X				
DCFA-1	Functional Architecture for AIS Applications	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				PL-2(1)	System Security Plan (Control Enhancement)				X		X	X	X		X	X	X		X	X
		I	I	I				PM-7	Enterprise Architecture	X	X	X	X				X				X			
		I	I	I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCHW-1	HW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCID-1	Interconnection Documentation	I	I	I				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-5(2)	Information System Documentation (Control Enhancement)			X					X			X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCII-1	IA Impact Assessment	I	I	I				CA-1	Security Assessment and Authorization Policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-3(2)	Configuration Change Control (Control Enhancement)		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				
		I	I	I				RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
DCIT-1	IA for IT Services	I	I	I				PS-7	Third-Party Personnel Security	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCMC-1	Mobile Code	I	I	I				SA-4	Acquisitions	X	X	X					X	X	X	X				
		I	I	I				SC-18	Mobile Code		X	X					X	X	X	X				
DCNR-1	Non-repudiation	I	I	I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				AU-10(5)	Non-repudiation (Control Enhancement)								X		X	X				
DCPA-1	Partitioning the Application	I	I	I				SC-2	Application Partitioning		X	X	X		X	X	X		X	X				
DCPD-1	Public Domain Software Controls	A	A	A				SA-6	Software Usage Restrictions	X	X	X	X	X	X	X	X	X	X	X				
DCPP-1	Ports, Protocols, and Services	A	A	A				CM-7(1)	Least Functionality (Control Enhancement)		X	X	X		X	X	X		X	X				
		A	A	A				SA-9	External Information System Services	X	X	X					X	X	X	X				
DCPR-1	CM Process	I	I	I				CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				CM-3	Configuration Change Control		X	X					X		X	X				
		I	I	I				CM-4	Security Impact Analysis	X	X	X					X		X	X				

Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C		CN				BL					C					I					A		
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL.	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
		I	I	I				CM-5	Access Restrictions for Change		X	X					X		X	X				
		I	I	I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
		I	I	I				CM-9	Configuration Management Plan		X	X					X		X	X				
DCSD-1	IA Documentation	A	A	A				PL-2	System Security Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
DCSL-1	System Library Management Controls	I	I	I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
DCSQ-1	Software Quality	I	I	I				CM-4(1)	Security Impact Analysis (Control Enhancement)			X					X			X				
		I	I	I				SA-11(1)	Developer Security Testing (Control Enhancement)								X							
		I	I	I				SA-4(3)	Acquisitions (Control Enhancement)								X		X	X				
		I	I	I				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
DCSS-1	System State Changes			I				CM-6	Configuration Settings	X	X	X					X	X	X	X				
				I				SI-6	Security Functionality Verification			X					X		X	X				
DCSW-1	SW Baseline	A	A	A				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		A	A	A				CM-8	Information System Component Inventory	X	X	X					X	X	X	X				
		A	A	A				SA-5	Information System Documentation	X	X	X					X	X	X	X				
EBCR-1	Connection Rules	A	A	A				AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
		A	A	A				CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBVC-1	VPN Controls	A	A	A				SI-4(10)	Information System Monitoring Tools and Techniques (Control Enhancement)				X		X	X	X		X	X				
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			I		I	I	AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
ECCD-1	Changes to Data			I				AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
ECIM-1	Instant Messaging	I	I	I				CM-2	Baseline Configuration	X	X	X					X	X	X	X				
		I	I	I				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		I	I	I				SC-15(2)	Collaborative Computing Devices (Control Enhancement)				X		X	X	X		X	X				
		I	I	I				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECND-1	Network Device Controls			I				CP-10	Information System Recovery and Reconstitution	X	X	X									X	X	X	X
				I				SA-5	Information System Documentation	X	X	X					X	X	X	X				
ECPA-1	Privileged Account Control	I	I	I				AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AC-2(7)	Account Management (Control Enhancement)				X		X	X	X		X	X				
ECPC-1	Production Code Change Controls			I				CM-5(5)	Access Restrictions for Change (Control Enhancement)								X							
ECRG-1	Audit Reduction and Report Generation	I	I	I				AU-7	Audit Reduction and Report Generation		X	X	X		X	X	X		X	X				
ECSC-1	Security Configuration Compliance	A	A	A				CM-6	Configuration Settings	X	X	X					X	X	X	X				
ECSD-1	Software Development Change Controls			I				CM-5	Access Restrictions for Change		X	X					X		X	X				
ECTB-1	Audit Trail Backup	I	I	I				AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I	I				AU-9(2)	Protection of Audit Information (Control Enhancement)												X			
ECTM-1	Transmission Integrity Controls			I				SC-8	Transmission Integrity		X	X					X	X	X	X				
				I				SI-7	Software and Information Integrity		X	X					X		X	X				
ECTP-1	Audit Trail Protection		I	I				AU-9	Protection of Audit Information	X	X	X	X	X	X	X	X	X	X	X				

Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III

DoDI 8500.2								NIST SP 800-53r3							CNSSI 1253											
		M	A	C		CN				BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL.	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
ECVI-1	Voice-over-IP (VoIP) Protection	A	A	A				CM-7	Least Functionality	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				SC-15	Collaborative Computing Devices	X	X	X	X	X	X	X								
		A	A	A				SC-19	Voice Over Internet Protocol		X	X	X		X	X	X		X	X				
		A	A	A				SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECVP-1	Virus Protection	A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
ECWN-1	Wireless Computing and Network	A	A	A				AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				AC-19	Access Control for Mobile Devices	X	X	X	X	X	X	X	X	X	X	X				
IAKM-1	Key Management			I				IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12(2)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-12(4)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-13(1)	Use of Cryptography (Control Enhancement)				X											
				I				SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
IATS-1	Token and Certificate Standards			I				IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
				I				SC-12(4)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
				I				SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
PEEL-1	Emergency Lighting			A				PE-12	Emergency Lighting	X	X	X									X	X	X	X
PEFD-1	Fire Detection			A				PE-13	Fire Protection	X	X	X									X	X	X	X
PEFI-1	Fire Inspection	A	A	A				PE-13	Fire Protection	X	X	X									X	X	X	X
		A	A	A				PE-13(4)	Fire Protection (Control Enhancement)												X		X	X
PEFS-1	Fire Suppression			A				PE-13	Fire Protection	X	X	X									X	X	X	X
PEHC-1	Humidity Controls			A				PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
				A				PE-14(2)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PEMS-1	Master Power Switch	A	A	A				PE-10	Emergency Shutoff		X	X									X		X	X
PESL-1	Screen Lock	I	I	I				AC-11	Session Lock		X	X	X	X	X	X	X	X	X	X				
		I	I	I				AC-11(1)	Session Lock (Control Enhancement)				X	X	X	X								
PETC-1	Temperature Controls			A				PE-14	Temperature and Humidity Controls	X	X	X									X	X	X	X
				A				PE-14(2)	Temperature and Humidity Controls (Control Enhancement)												X		X	X
PETN-1	Environmental Control Training	A	A	A				PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PEVR-1	Voltage Regulators	A	A	A				PE-9(2)	Power Equipment and Power Cabling (Control Enhancement)												X		X	X
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	A	A	A				PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
		A	A	A				PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIIR-1	Incident Response Planning		A	A				IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix D – DoDI 8500.2 Security Control Mapping for Mission Assurance Category III

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253											
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL.	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
			A	A				IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-3	Incident Response Testing and Exercises		X	X	X		X	X	X		X	X	X		X	X
			A	A				IR-4	Incident Handling	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			A	A				IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VIVM-1	Vulnerability Management	A	A	A				CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
		A	A	A				RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		A	A	A				SI-2	Flaw Remediation	X	X	X					X	X	X	X				
		A	A	A				SI-3	Malicious Code Protection	X	X	X					X	X	X	X				
		A	A	A				SI-5	Security Alerts, Advisories, and Directives	X	X	X					X	X	X	X				

Appendix E – DoDI 8500.2 Security Control Mapping for Systems Processing Classified Information

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
DCAS-1	Acquisition Standards				C	C	C	SA-4(6)	Acquisitions (Control Enhancement)								X		X	X				
					C	C	C	SA-4(7)	Acquisitions (Control Enhancement)								X		X	X				
DCSR-3	Specified Robustness – High				C			SA-4	Acquisitions	X	X	X					X	X	X	X				
DCSS-2	System State Changes	I	I		I			SI-6	Security Functionality Verification			X					X		X	X				
EBBD-3	Boundary Defense				C			AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
					C			CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
					C			CA-3(2)	Information System Connections (Control Enhancement)				X	X	X	X								
					C			SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
					C			SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBRP-1	Remote Access for Privileged Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(7)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
					C	C		MA-4	Non-Local Maintenance	X	X	X					X	X	X	X				
					C	C		MA-4(1)	Non-Local Maintenance (Control Enhancement)		X	X					X		X	X				
					C	C		MA-4(6)	Non-Local Maintenance (Control Enhancement)				X				X							
EBRU-1	Remote Access for User Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
					C	C		IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-17	Alternate Work Site		X	X	X		X	X	X		X	X	X		X	X
					C	C		SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECAD-1	Affiliation Display				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
ECAN-1	Access for Need-to-Know				C	C		AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		AC-2(6)	Account Management (Control Enhancement)				X				X							
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(3)	Access Enforcement (Control Enhancement)				X				X							
					C	C		AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECAR-3	Audit Record Content – Classified Systems Audit of Security Label Changes				C			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	I	I		I			AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
		I	I		I			AU-5	Response to Audit Processing Failures	X	X	X									X	X	X	X
		I	I		I			AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			IR-4(5)	Incident Handling (Control Enhancement)				X				X							
ECCD-2	Changes to Data	I	I		I			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
		I	I		I			AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				

Appendix E – DoDI 8500.2 Security Control Mapping for Systems Processing Classified Information

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
ECCM-1	COMSEC				C			SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			SC-8	Transmission Integrity		X	X					X	X	X	X				
					C			SC-9	Transmission Confidentiality		X	X	X	X	X	X								
ECCR-2	Encryption for Confidentiality (Data at Rest)				C			AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C			MP-4	Media Storage		X	X	X	X	X	X								
					C			SC-13(3)	Use of Cryptography (Control Enhancement)				X											
					C			SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				
ECCR-3	Encryption for Confidentiality (Data at Rest)				C			MP-4	Media Storage		X	X	X	X	X	X								
					C			SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								
					C			SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				
ECCT-2	Encryption for Confidentiality (Data at Transmit)				C			SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECIC-1	Interconnections among DoD Systems and Enclaves				C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(4)	Access Enforcement (Control Enhancement)				X	X	X	X	X	X	X	X				
					C	C		AC-4(14)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		AC-4(15)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
ECLC-1	Audit Record Content – Classified Systems Audit of Security Label Changes				C			AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
					C			AU-8	Time Stamps	X	X	X					X	X	X	X				
ECLO-2	Logon				C			AC-10	Concurrent Session Control			X					X		X	X				
					C			AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	X	X		X	X	X
					C			AC-9	Previous Logon (Access) Notification								X		X	X				
ECLP-1	Least Privilege				C	C	C	AC-5	Separation of Duties		X	X	X		X	X	X		X	X				
					C	C	C	AC-6	Least Privilege		X	X	X		X	X	X		X	X				
ECML-1	Marking and Labeling				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
					C	C		MP-3	Media Marking		X	X	X	X	X	X								
ECNK-1	Encryption for Need-To-Know				C	C		SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECNK-2	Encryption for Need-To-Know				C			SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECRC-1	Resource Control				C	C		SC-4	Information In Shared Resources		X	X	X		X	X								
ECRR-1	Audit Record Retention				I	I	I	AU-11	Audit Record Retention	X	X	X									X	X	X	X
ECTC-1	Tempest Controls				C	C		AC-18(5)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
					C	C		PE-19	Information Leakage				X		X	X			X	X				
ECWM-1	Warning Message				C	C	C	AC-8	System Use Notification	X	X	X	X	X	X	X	X	X	X	X				
IAAC-1	Account Control				C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
IAGA-1	Group Authentication				C	C		IA-2(5)	User Identification and Authentication (Organizational Users) (Control Enhancement)				X		X	X	X		X	X				
					C	C		IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
					C	C		IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
IAIA-2	Individual Identification and Authentication				C			IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				

Appendix E – DoDI 8500.2 Security Control Mapping for Systems Processing Classified Information

DoDI 8500.2								NIST SP 800-53r3												CNSSI 1253							
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
					C			IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
					C			IA-5(1)	Authenticator Management (Control Enhancement)	X	X	X	X		X	X	X		X	X				
					C			IA-5(3)	Authenticator Management (Control Enhancement)								X		X	X				
					C			IA-5(5)	Authenticator Management (Control Enhancement)				X				X							
					C			IA-5(6)	Authenticator Management (Control Enhancement)				X	X	X	X	X	X	X	X				
IAKM-3	Key Management				I			IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-12	Cryptographic Key Establishment and Management	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				X				X							
					I			SC-13	Use of Cryptography	X	X	X	X	X	X	X	X	X	X	X				
					I			SC-13(2)	Use of Cryptography (Control Enhancement)				X	X	X	X								
					I			SC-17	Public Key Infrastructure Certificates		X	X	X		X	X	X		X	X				
PECF-2	Access to Computing Facilities				C			PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-2(3)	Physical Access Authorizations (Control Enhancement)				X	X	X	X								
PECS-2	Clearing and Sanitizing				C			MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
					C			MP-6(5)	Media Sanitization (Control Enhancement)				X	X	X	X								
PEDD-1	Destruction				C			MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
					C			MP-6(6)	Media Sanitization (Control Enhancement)				X	X	X	X								
PEDI-1	Data Interception				I	I		MP-2	Media Access	X	X	X	X	X	X	X								
					I	I		PE-5	Access Control for Output Devices		X	X	X		X	X								
PEPF-2	Physical Protection of Facilities				C			MP-2	Media Access	X	X	X	X	X	X	X								
					C			PE-2(2)	Physical Access Authorizations (Control Enhancement)				X				X							
					C			PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-3(3)	Physical Access Control (Control Enhancement)				X	X	X	X	X	X	X	X				
					C			PE-5	Access Control for Output Devices		X	X	X		X	X								
					C			PE-6	Monitoring Physical Access	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			PE-6(1)	Monitoring Physical Access (Control Enhancement)		X	X									X		X	X
					C			PE-8	Access Records	X	X	X	X	X	X	X	X	X	X	X				
PEPS-1	Physical Security Testing				C	C		CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
					C	C		PE-3(6)	Physical Access Control (Control Enhancement)								X			X				
PESP-1	Workplace Security Procedures				C	C		MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		SI-12	Information Output Handling and Retention	X	X	X	X	X	X	X	X	X	X	X				
PESS-1	Storage				C	C		MP-4	Media Storage		X	X	X	X	X	X								
PEVC-1	Visitor Control to Computing Facilities				C	C		PE-7	Visitor Control	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-8	Access Records	X	X	X	X	X	X	X	X	X	X	X				
PRAS-2	Access to Information				C			AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix E – DoDI 8500.2 Security Control Mapping for Systems Processing Classified Information

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C	CN					BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
					C			PS-3	Personnel Screening	X	X	X	X	X	X	X	X	X	X	X				
					C			PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C			PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								
PRMP-2	Maintenance Personnel				C			MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(1)	Maintenance Personnel (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(2)	Maintenance Personnel (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
					C			MA-5(3)	Maintenance Personnel (Control Enhancement)				X				X				X			
PRNK-1	Access to Need-to-Know Information				C	C	C	AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
					C	C	C	PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								
PRTN-1	Information Assurance Training				I	I		AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-2	Security Awareness	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-3	Security Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		CP-3	Contingency Training	X	X	X									X	X	X	X
					I	I		IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix F – DoDI 8500.2 Security Control Mapping for Systems Processing Sensitive Information

DoDI 8500.2								NIST SP 800-53r3					CNSSI 1253													
		M	A	C	CN					BL			C				I				A					
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
DCAS-1	Acquisition Standards				C	C	C	SA-4(6)	Acquisitions (Control Enhancement)								X		X	X				
					C	C	C	SA-4(7)	Acquisitions (Control Enhancement)								X		X	X				
DCSR-2	Specified Robustness - Medium					C		SA-4	Acquisitions	X	X	X					X	X	X	X				
EBBD-2	Boundary Defense					C		AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
						C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
						C		CA-3(1)	Information System Connections (Control Enhancement)				X											
						C		SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
						C		SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBPW-1	Public WAN Connection					C	C	CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
						C	C	SC-14	Public Access Protections	X	X	X					X	X	X	X	X	X	X	X
						C	C	SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
EBRP-1	Remote Access for Privileged Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(7)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
					C	C		MA-4	Non-Local Maintenance	X	X	X					X	X	X	X				
					C	C		MA-4(1)	Non-Local Maintenance (Control Enhancement)		X	X					X		X	X				
					C	C		MA-4(6)	Non-Local Maintenance (Control Enhancement)				X				X							
EBRU-1	Remote Access for User Functions				C	C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-17(2)	Remote Access (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
					C	C		IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-17	Alternate Work Site		X	X	X		X	X	X		X	X	X		X	X
					C	C		SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECAD-1	Affiliation Display				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
ECAN-1	Access for Need-to-Know				C	C		AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		AC-2(6)	Account Management (Control Enhancement)				X				X							
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(3)	Access Enforcement (Control Enhancement)				X				X							
					C	C		AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
ECAR-2	Audit Record Content – Sensitive Systems					C		AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
						C		AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
						C		AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			I		I	I	AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
ECCR-1	Encryption for Confidentiality (Data at Rest)					C		MP-4	Media Storage		X	X	X	X	X	X								
						C		SC-13(1)	Use of Cryptography (Control Enhancement)				X											

Appendix F – DoDI 8500.2 Security Control Mapping for Systems Processing Sensitive Information

DoDI 8500.2								NIST SP 800-53r3								CNSSI 1253											
		M	A	C		CN				BL			C				I				A						
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
						C		SC-28	Protection of Information at Rest		X	X	X		X	X	X		X	X				
ECCT-1	Encryption for Confidentiality (Data at Transmit)					C		AC-17	Remote Access	X	X	X	X	X	X	X	X	X	X	X				
						C		AC-18	Wireless Access Restrictions	X	X	X	X	X	X	X	X	X	X	X				
						C		SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECIC-1	Interconnections among DoD Systems and Enclaves				C	C		AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C		AC-3(4)	Access Enforcement (Control Enhancement)				X	X	X	X	X	X	X	X				
					C	C		AC-4(14)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		AC-4(15)	Information Flow Enforcement (Control Enhancement)				X				X							
					C	C		CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
ECLO-1	Logon					C		AC-10	Concurrent Session Control			X					X		X	X				
						C		AC-7	Unsuccessful Login Attempts	X	X	X	X	X	X	X	X	X	X	X		X	X	X
ECLP-1	Least Privilege				C	C	C	AC-5	Separation of Duties		X	X	X		X	X	X		X	X				
					C	C	C	AC-6	Least Privilege		X	X	X		X	X	X		X	X				
ECML-1	Marking and Labeling				C	C		AC-16	Security Attributes				X	X	X	X	X	X	X	X				
					C	C		MP-3	Media Marking		X	X	X	X	X	X								
ECMT-1	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECMT-2	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECNK-1	Encryption for Need-To-Know				C	C		SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	X	X	X	X								
ECRC-1	Resource Control				C	C		SC-4	Information In Shared Resources		X	X	X		X	X								
ECRR-1	Audit Record Retention				I	I	I	AU-11	Audit Record Retention	X	X	X									X	X	X	X
ECTC-1	Tempest Controls				C	C		AC-18(5)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
					C	C		PE-19	Information Leakage				X		X	X			X	X				
ECWM-1	Warning Message				C	C	C	AC-8	System Use Notification	X	X	X	X	X	X	X	X	X	X	X				
IAAC-1	Account Control				C	C		AC-2	Account Management				X	X	X	X	X	X	X	X				
					C	C		PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
IAGA-1	Group Authentication				C	C		IA-2(5)	User Identification and Authentication (Organizational Users) (Control Enhancement)				X		X	X	X		X	X				
					C	C		IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
					C	C		IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
IAIA-1	Individual Identification and Authentication					C		IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-2	User Identification and Authentication (Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-4	Identifier Management	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-5	Authenticator Management	X	X	X	X	X	X	X	X	X	X	X				
						C		IA-5(1)	Authenticator Management (Control Enhancement)	X	X	X	X		X	X	X		X	X				
						C		IA-5(3)	Authenticator Management (Control Enhancement)								X		X	X				
						C		IA-5(5)	Authenticator Management (Control Enhancement)				X				X							

Appendix F – DoDI 8500.2 Security Control Mapping for Systems Processing Sensitive Information

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253											
		M	A	C		CN				BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
						C		IA-5(6)	Authenticator Management (Control Enhancement)				X	X	X	X	X	X	X	X				
PECF-1	Access to Computing Facilities					C		PE-2	Physical Access Authorizations	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PECS-1	Clearing and Sanitizing					C		MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		MP-6	Media Sanitization and Disposal	X	X	X	X	X	X	X								
						C		MP-6(4)	Media Sanitization (Control Enhancement)				X											
PEDI-1	Data Interception				I	I		MP-2	Media Access	X	X	X	X	X	X	X								
					I	I		PE-5	Access Control for Output Devices		X	X	X		X	X								
PEPF-1	Physical Protection of Facilities					C		MP-2	Media Access	X	X	X	X	X	X	X								
						C		PE-3	Physical Access Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		PE-5	Access Control for Output Devices		X	X	X		X	X								
PEPS-1	Physical Security Testing				C	C		CA-2	Security Assessments	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
					C	C		PE-3(6)	Physical Access Control (Control Enhancement)								X			X				
PESP-1	Workplace Security Procedures				C	C		MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					C	C		SI-12	Information Output Handling and Retention	X	X	X	X	X	X	X	X	X	X	X				
PESS-1	Storage				C	C		MP-4	Media Storage		X	X	X	X	X	X								
PEVC-1	Visitor Control to Computing Facilities				C	C		PE-7	Visitor Control	X	X	X	X	X	X	X	X	X	X	X				
					C	C		PE-8	Access Records	X	X	X	X	X	X	X	X	X	X	X				
PRAS-1	Access to Information					C		AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C		PS-3	Personnel Screening	X	X	X	X	X	X	X	X	X	X	X				
						C		PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
						C		PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
PRMP-1	Maintenance Personnel					C	C	MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C	C	MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PRNK-1	Access to Need-to-Know Information				C	C	C	AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
					C	C	C	PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								
PRTN-1	Information Assurance Training				I	I		AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-2	Security Awareness	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		AT-3	Security Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
					I	I		CP-3	Contingency Training	X	X	X									X	X	X	X
					I	I		IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Appendix G – DoDI 8500.2 Security Control Mapping for Systems Processing Public Information

DoDI 8500.2								NIST SP 800-53r3						CNSSI 1253											
		M	A	C	CN					BL			C				I				A			
CONTROL	CONTROL NAME	I	II	III	CL	SN	PB	CONTROL	CONTROL NAME	L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
DCAS-1	Acquisition Standards				C	C	C	SA-4(6)	Acquisitions (Control Enhancement)								X		X	X				
					C	C	C	SA-4(7)	Acquisitions (Control Enhancement)								X		X	X				
DCSR-1	Specified Robustness - Basic						C	SA-4	Acquisitions	X	X	X					X	X	X	X				
EBBD-1	Boundary Defense						C	AC-4	Information Flow Enforcement		X	X	X		X	X	X		X	X				
							C	CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
							C	CA-3(1)	Information System Connections (Control Enhancement)				X											
EBBD-1	Boundary Defense						C	SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
							C	SI-4	Information System Monitoring Tools and Techniques		X	X					X		X	X				
EBPW-1	Public WAN Connection					C	C	CA-3	Information System Connections	X	X	X	X	X	X	X	X	X	X	X				
						C	C	SC-14	Public Access Protections	X	X	X					X	X	X	X	X	X	X	X
						C	C	SC-7	Boundary Protection	X	X	X	X	X	X	X	X	X	X	X				
ECAR-1	Audit Record Content – Public Systems						C	AU-2	Auditable Events	X	X	X	X	X	X	X	X	X	X	X				
							C	AU-3	Content of Audit Records	X	X	X	X	X	X	X	X	X	X	X				
							C	AU-8	Time Stamps	X	X	X					X	X	X	X				
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting			I		I	I	AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-12	Audit Generation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
				I		I	I	AU-6	Audit Review, Analysis, and Reporting	X	X	X	X	X	X	X	X	X	X	X				
ECLP-1	Least Privilege				C	C	C	AC-5	Separation of Duties		X	X	X		X	X	X		X	X				
					C	C	C	AC-6	Least Privilege		X	X	X		X	X	X		X	X				
ECMT-1	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECMT-2	Conformance Monitoring and Testing					C	C	CA-2(2)	Security Assessments (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
						C	C	CA-7(2)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
						C	C	RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ECRR-1	Audit Record Retention				I	I	I	AU-11	Audit Record Retention	X	X	X									X	X	X	X
ECWM-1	Warning Message				C	C	C	AC-8	System Use Notification	X	X	X	X	X	X	X	X	X	X	X				
PRMP-1	Maintenance Personnel					C	C	MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
						C	C	MA-5	Maintenance Personnel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PRNK-1	Access to Need-to-Know Information				C	C	C	AC-3	Access Enforcement	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6	Access Agreements	X	X	X	X	X	X	X	X	X	X	X				
					C	C	C	PS-6(1)	Access Agreements (Control Enhancement)				X		X	X	X		X	X				
					C	C	C	PS-6(2)	Access Agreements (Control Enhancement)				X	X	X	X								

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253														
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							AC-14	Permitted Actions without Identification or Authentication	X	X	X	X	X	X	X	X	X	X	X				
							AC-14(1)	Permitted Actions without Identification or Authentication (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-16(1)	Security Attributes (Control Enhancement)				X				X							
							AC-16(2)	Security Attributes (Control Enhancement)								X							
							AC-16(3)	Security Attributes (Control Enhancement)								X							
							AC-16(4)	Security Attributes (Control Enhancement)				X	X	X	X	X	X	X	X				
							AC-16(5)	Security Attributes (Control Enhancement)				X											
							AC-17(1)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-17(3)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-17(4)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-17(5)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-17(6)	Remote Access (Control Enhancement)		X	X	X		X	X								
							AC-17(8)	Remote Access (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-18(1)	Wireless Access Restrictions (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-18(2)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
							AC-18(3)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
							AC-18(4)	Wireless Access Restrictions (Control Enhancement)			X	X		X	X	X		X	X				
							AC-19(1)	Access Control for Mobile Devices (Control Enhancement)		X	X	X		X	X								
							AC-19(2)	Access Control for Mobile Devices (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-19(3)	Access Control for Mobile Devices (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-19(4)	Access Control for Mobile Devices (Control Enhancement)				X	X	X	X								
							AC-2(1)	Account Management (Control Enhancement)	X	X	X	X		X	X	X		X	X				
							AC-2(2)	Account Management (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-2(3)	Account Management (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-2(4)	Account Management (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-2(5)	Account Management (Control Enhancement)				X				X							
							AC-20	Use of External Information Systems	X	X	X	X	X	X	X	X	X	X	X				
							AC-20(1)	Use of External Information Systems (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-20(2)	Use of External Information Systems (Control Enhancement)		X	X	X		X	X								
							AC-21	User-Based Collaboration and Information Sharing				X											
							AC-21(1)	User-Based Collaboration and Information Sharing (Control Enhancement)				X											
							AC-22	Publicly Accessible Content	X	X	X	X	X	X	X								
							AC-3(2)	Access Enforcement (Control Enhancement)				X				X							
							AC-3(5)	Access Enforcement (Control Enhancement)				X				X							
							AC-3(6)	Access Enforcement (Control Enhancement)				X				X							
							AC-4(1)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(10)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(11)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(12)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(13)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(16)	Information Flow Enforcement (Control Enhancement)				X				X							

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A					
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							AC-4(17)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(2)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(3)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(4)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(5)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(6)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(7)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(8)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-4(9)	Information Flow Enforcement (Control Enhancement)				X				X							
							AC-6(1)	Least Privilege (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-6(2)	Least Privilege (Control Enhancement)		X	X	X		X	X	X		X	X				
							AC-6(3)	Least Privilege (Control Enhancement)				X				X							
							AC-6(4)	Least Privilege (Control Enhancement)				X				X							
							AC-6(5)	Least Privilege (Control Enhancement)				X		X	X	X		X	X				
							AC-6(6)	Least Privilege (Control Enhancement)				X				X							
							AC-7(1)	Unsuccessful Login Attempts (Control Enhancement)				X		X	X	X		X	X				
							AC-7(2)	Unsuccessful Login Attempts (Control Enhancement)				X											
							AC-9(1)	Previous Logon (Access) Notification (Control Enhancement)								X							
							AC-9(2)	Previous Logon (Access) Notification (Control Enhancement)								X							
							AC-9(3)	Previous Logon (Access) Notification (Control Enhancement)								X							
							AT-2(1)	Security Awareness (Control Enhancement)				X				X				X			
							AT-3(1)	Security Training (Control Enhancement)												X			
							AT-3(2)	Security Training (Control Enhancement)				X		X	X	X		X	X	X		X	X
							AT-4	Security Training Records	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
							AT-5	Contacts with Security Groups and Associations				X				X				X			
							AU-10	Non-repudiation			X					X		X	X				
							AU-10(1)	Non-repudiation (Control Enhancement)								X							
							AU-10(2)	Non-repudiation (Control Enhancement)								X							
							AU-10(3)	Non-repudiation (Control Enhancement)								X							
							AU-10(4)	Non-repudiation (Control Enhancement)								X							
							AU-12(1)	Audit Generation (Control Enhancement)			X					X			X				
							AU-12(2)	Audit Generation (Control Enhancement)								X							
							AU-13	Monitoring For Information Disclosure				X											
							AU-14	Session Audit												X			
							AU-14(1)	Session Audit (Control Enhancement)												X			
							AU-2(3)	Auditable Events (Control Enhancement)		X	X	X		X	X	X		X	X				
							AU-2(4)	Auditable Events (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
							AU-3(1)	Content of Audit Records (Control Enhancement)		X	X	X		X	X	X		X	X				
							AU-3(2)	Content of Audit Records (Control Enhancement)			X	X			X	X			X				
							AU-4	Audit Storage Capacity	X	X	X									X	X	X	X
							AU-5(1)	Response to Audit Processing Failures (Control Enhancement)			X									X			X

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							AU-5(2)	Response to Audit Processing Failures (Control Enhancement)			X									X			X
							AU-5(3)	Response to Audit Processing Failures (Control Enhancement)												X			
							AU-5(4)	Response to Audit Processing Failures (Control Enhancement)				X				X							
							AU-6(1)	Audit Review, Analysis, and Reporting (Control Enhancement)			X	X			X	X			X				
							AU-6(3)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-6(4)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-6(5)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-6(6)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-6(7)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-6(8)	Audit Review, Analysis, and Reporting (Control Enhancement)				X		X	X	X		X	X				
							AU-6(9)	Audit Review, Analysis, and Reporting (Control Enhancement)				X				X							
							AU-7(1)	Audit Reduction and Report Generation (Control Enhancement)		X	X	X		X	X	X		X	X				
							AU-8(1)	Time Stamps (Control Enhancement)		X	X					X		X	X				
							AU-9(1)	Protection of Audit Information (Control Enhancement)								X							
							AU-9(3)	Protection of Audit Information (Control Enhancement)								X							
							AU-9(4)	Protection of Audit Information (Control Enhancement)								X							
							CA-5	Plan of Action and Milestones	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
							CA-5(1)	Plan of Action and Milestones (Control Enhancement)				X				X				X			
							CA-6	Security Authorization	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
							CA-7(1)	Continuous Monitoring (Control Enhancement)				X		X	X	X		X	X	X		X	X
							CM-2(1)	Baseline Configuration (Control Enhancement)		X	X					X		X	X				
							CM-2(2)	Baseline Configuration (Control Enhancement)			X					X			X				
							CM-2(3)	Baseline Configuration (Control Enhancement)		X	X					X		X	X				
							CM-2(4)	Baseline Configuration (Control Enhancement)		X						X		X					
							CM-2(5)	Baseline Configuration (Control Enhancement)			X					X			X				
							CM-2(6)	Baseline Configuration (Control Enhancement)			X					X			X				
							CM-3(1)	Configuration Change Control (Control Enhancement)			X					X			X				
							CM-3(3)	Configuration Change Control (Control Enhancement)								X							
							CM-5(1)	Access Restrictions for Change (Control Enhancement)			X					X		X	X				
							CM-5(2)	Access Restrictions for Change (Control Enhancement)			X					X			X				
							CM-5(3)	Access Restrictions for Change (Control Enhancement)			X					X			X				
							CM-5(4)	Access Restrictions for Change (Control Enhancement)								X							
							CM-5(6)	Access Restrictions for Change (Control Enhancement)								X		X	X				
							CM-5(7)	Access Restrictions for Change (Control Enhancement)								X							
							CM-6(1)	Configuration Settings (Control Enhancement)			X					X			X				
							CM-6(2)	Configuration Settings (Control Enhancement)			X					X			X				
							CM-6(3)	Configuration Settings (Control Enhancement)		X	X					X		X	X				
							CM-7(2)	Least Functionality (Control Enhancement)			X	X			X	X			X				
							CM-7(3)	Least Functionality (Control Enhancement)				X		X	X	X		X	X				
							CM-8(1)	Information System Component Inventory (Control Enhancement)		X	X					X		X	X				
							CM-8(2)	Information System Component Inventory (Control Enhancement)			X					X			X				

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253														
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							CM-8(3)	Information System Component Inventory (Control Enhancement)			X					X			X				
							CM-8(4)	Information System Component Inventory (Control Enhancement)			X					X			X				
							CM-8(5)	Information System Component Inventory (Control Enhancement)		X	X					X		X	X				
							CM-8(6)	Information System Component Inventory (Control Enhancement)								X							
							CM-9(1)	Configuration Management Plan (Control Enhancement)								X							
							CP-10(3)	Information System Recovery and Reconstitution (Control Enhancement)		X	X									X		X	X
							CP-10(4)	Information System Recovery and Reconstitution (Control Enhancement)			X					X			X	X			X
							CP-10(5)	Information System Recovery and Reconstitution (Control Enhancement)												X			
							CP-10(6)	Information System Recovery and Reconstitution (Control Enhancement)								X				X		X	X
							CP-2(1)	Contingency Plan (Control Enhancement)		X	X									X		X	X
							CP-2(2)	Contingency Plan (Control Enhancement)			X									X			X
							CP-2(6)	Contingency Plan (Control Enhancement)												X			
							CP-3(1)	Contingency Training (Control Enhancement)			X									X			X
							CP-3(2)	Contingency Training (Control Enhancement)												X			
							CP-4(1)	Contingency Plan Testing and Exercises (Control Enhancement)		X	X									X		X	X
							CP-4(2)	Contingency Plan Testing and Exercises (Control Enhancement)			X									X			X
							CP-4(3)	Contingency Plan Testing and Exercises (Control Enhancement)												X			
							CP-4(4)	Contingency Plan Testing and Exercises (Control Enhancement)			X									X		X	X
							CP-6(1)	Alternate Storage Site (Control Enhancement)		X	X									X		X	X
							CP-6(2)	Alternate Storage Site (Control Enhancement)			X									X			X
							CP-6(3)	Alternate Storage Site (Control Enhancement)		X	X									X		X	X
							CP-7(1)	Alternate Processing Site (Control Enhancement)		X	X									X		X	X
							CP-7(2)	Alternate Processing Site (Control Enhancement)		X	X									X		X	X
							CP-7(3)	Alternate Processing Site (Control Enhancement)		X	X									X		X	X
							CP-8	Telecommunications Services		X	X	X				X				X		X	X
							CP-8(1)	Telecommunications Services (Control Enhancement)		X	X									X		X	X
							CP-8(2)	Telecommunications Services (Control Enhancement)		X	X									X		X	X
							CP-8(3)	Telecommunications Services (Control Enhancement)			X									X			X
							CP-8(4)	Telecommunications Services (Control Enhancement)			X									X			X
							CP-9(1)	Information System Backup (Control Enhancement)		X	X					X		X	X	X		X	X
							CP-9(2)	Information System Backup (Control Enhancement)			X					X			X	X			X
							CP-9(5)	Information System Backup (Control Enhancement)												X			
							IA-2(1)	User Identification and Authentication (Organizational Users) (Control Enhancement)	X	X	X	X	X	X	X	X	X	X	X				
							IA-2(2)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X	X		X	X	X		X	X				
							IA-2(3)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X	X		X	X	X		X	X				
							IA-2(4)	User Identification and Authentication (Organizational Users) (Control Enhancement)				X			X	X			X				
							IA-2(6)	User Identification and Authentication (Organizational Users) (Control Enhancement)															
							IA-2(7)	User Identification and Authentication (Organizational Users) (Control Enhancement)				X				X							
							IA-2(8)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X	X	X	X	X	X	X	X	X				
							IA-2(9)	User Identification and Authentication (Organizational Users) (Control Enhancement)			X	X		X	X	X		X	X				
							IA-3	Device Identification and Authentication		X	X	X		X	X	X		X	X				

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A					
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							IA-3(1)	Device Identification and Authentication (Control Enhancement)				X				X							
							IA-3(2)	Device Identification and Authentication (Control Enhancement)				X				X							
							IA-3(3)	Device Identification and Authentication (Control Enhancement)				X				X							
							IA-4(1)	Identifier Management (Control Enhancement)				X				X							
							IA-4(2)	Identifier Management (Control Enhancement)								X							
							IA-4(3)	Identifier Management (Control Enhancement)								X							
							IA-4(4)	Identifier Management (Control Enhancement)				X		X	X	X		X	X				
							IA-4(5)	Identifier Management (Control Enhancement)				X				X							
							IA-5(2)	Authenticator Management (Control Enhancement)		X	X					X		X	X				
							IA-5(4)	Authenticator Management (Control Enhancement)				X		X	X	X		X	X				
							IA-5(7)	Authenticator Management (Control Enhancement)				X		X	X								
							IA-5(8)	Authenticator Management (Control Enhancement)				X				X							
							IA-6	Authenticator Feedback	X	X	X	X	X	X	X								
							IA-7	Cryptographic Module Authentication	X	X	X	X	X	X	X	X	X	X	X				
							IA-8	Identification and Authentication (Non-Organizational Users)	X	X	X	X	X	X	X	X	X	X	X				
							IR-2(1)	Incident Response Training (Control Enhancement)			X	X			X	X			X	X			X
							IR-2(2)	Incident Response Training (Control Enhancement)			X	X			X	X			X	X			X
							IR-3(1)	Incident Response Testing and Exercises (Control Enhancement)			X	X			X	X			X	X			X
							IR-4(1)	Incident Handling (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
							IR-4(2)	Incident Handling (Control Enhancement)				X				X				X			
							IR-4(3)	Incident Handling (Control Enhancement)				X				X				X			
							IR-4(4)	Incident Handling (Control Enhancement)				X				X				X			
							IR-5(1)	Incident Monitoring (Control Enhancement)			X	X			X	X			X	X			X
							IR-6(1)	Incident Reporting (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
							IR-6(2)	Incident Reporting (Control Enhancement)				X				X				X			
							IR-7(1)	Incident Response Assistance (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
							IR-7(2)	Incident Response Assistance (Control Enhancement)				X				X				X			
							MA-2(1)	Controlled Maintenance (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
							MA-2(2)	Controlled Maintenance (Control Enhancement)			X	X			X	X			X	X			X
							MA-3	Maintenance Tools		X	X					X	X	X	X	X	X	X	X
							MA-3(1)	Maintenance Tools (Control Enhancement)		X	X					X		X	X	X		X	X
							MA-3(2)	Maintenance Tools (Control Enhancement)		X	X					X		X	X	X		X	X
							MA-3(3)	Maintenance Tools (Control Enhancement)			X	X	X	X	X								
							MA-3(4)	Maintenance Tools (Control Enhancement)								X							
							MA-4(2)	Non-Local Maintenance (Control Enhancement)		X	X					X		X	X				
							MA-4(3)	Non-Local Maintenance (Control Enhancement)			X	X			X	X			X	X			
							MA-4(4)	Non-Local Maintenance (Control Enhancement)				X				X							
							MA-4(5)	Non-Local Maintenance (Control Enhancement)								X							
							MA-4(7)	Non-Local Maintenance (Control Enhancement)								X							
							MA-5(4)	Maintenance Personnel (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
							MP-2(1)	Media Access (Control Enhancement)		X	X	X		X	X	X		X	X				

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253											
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							MP-2(2)	Media Access (Control Enhancement)				X				X							
							MP-4(1)	Media Storage (Control Enhancement)				X	X	X	X								
							MP-5	Media Transport		X	X	X		X	X	X		X	X				
							MP-5(2)	Media Transport (Control Enhancement)		X	X	X		X	X	X		X	X				
							MP-5(3)	Media Transport (Control Enhancement)			X	X			X	X			X				
							MP-5(4)	Media Transport (Control Enhancement)		X	X	X		X	X	X		X	X				
							MP-6(1)	Media Sanitization (Control Enhancement)			X	X			X								
							MP-6(2)	Media Sanitization (Control Enhancement)			X	X			X								
							MP-6(3)	Media Sanitization (Control Enhancement)			X	X			X								
							PE-11	Emergency Power		X	X									X		X	X
							PE-15	Water Damage Protection	X	X	X									X	X	X	X
							PE-15(1)	Water Damage Protection (Control Enhancement)			X									X			X
							PE-16	Delivery and Removal	X	X	X	X	X	X	X					X	X	X	X
							PE-18	Location of Information System Components		X	X									X		X	X
							PE-18(1)	Location of Information System Components (Control Enhancement)			X									X			X
							PE-19(1)	Information Leakage (Control Enhancement)				X		X	X			X	X				
							PE-2(1)	Physical Access Authorizations (Control Enhancement)				X				X				X			
							PE-3(1)	Physical Access Control (Control Enhancement)			X	X			X	X			X				
							PE-3(2)	Physical Access Control (Control Enhancement)				X	X	X	X								
							PE-3(4)	Physical Access Control (Control Enhancement)				X				X							
							PE-3(5)	Physical Access Control (Control Enhancement)								X							
							PE-4	Access Control for Transmission Medium		X	X	X		X	X	X		X	X				
							PE-6(2)	Monitoring Physical Access (Control Enhancement)			X	X			X	X			X	X			X
							PE-7(1)	Visitor Control (Control Enhancement)		X	X	X		X	X	X		X	X				
							PE-7(2)	Visitor Control (Control Enhancement)				X				X							
							PE-8(1)	Access Records (Control Enhancement)			X									X			X
							PE-8(2)	Access Records (Control Enhancement)			X									X			X
							PE-9	Power Equipment and Power Cabling		X	X									X		X	X
							PE-9(1)	Power Equipment and Power Cabling (Control Enhancement)												X			
							PL-2(2)	System Security Plan (Control Enhancement)				X		X	X	X		X	X	X		X	X
							PL-4(1)	Rules of Behavior (Control Enhancement)				X											
							PL-5	Privacy Impact Assessment	X	X	X	X	X	X	X								
							PL-6	Security-Related Activity Planning		X	X	X		X	X	X		X	X	X		X	X
							PM-1	Information Security Program Plan	X	X	X	X				X				X			
							PM-10	Security Authorization Process	X	X	X	X				X				X			
							PM-11	Mission/Business Process Definition	X	X	X	X				X				X			
							PM-2	Senior Information Security Officer	X	X	X	X				X				X			
							PM-3	Information Security Resources	X	X	X	X				X				X			
							PM-4	Plan of Action and Milestones Process	X	X	X	X				X				X			
							PM-5	Information System Inventory	X	X	X	X				X				X			
							PM-6	Information Security Measures of Performance	X	X	X	X				X				X			

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3						CNSSI 1253														
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							PM-8	Critical Infrastructure Plan	X	X	X	X				X				X			
							PM-9	Risk Management Strategy	X	X	X	X				X				X			
							PS-2	Position Categorization	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
							PS-3(1)	Personnel Screening (Control Enhancement)				X	X	X	X								
							PS-3(2)	Personnel Screening (Control Enhancement)				X	X	X	X								
							RA-2	Security Categorization	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
							RA-5(1)	Vulnerability Scanning (Control Enhancement)		X	X	X		X	X	X		X	X	X		X	X
							RA-5(2)	Vulnerability Scanning (Control Enhancement)			X	X		X	X	X		X	X	X		X	X
							RA-5(3)	Vulnerability Scanning (Control Enhancement)			X	X			X	X			X	X			X
							RA-5(4)	Vulnerability Scanning (Control Enhancement)			X	X			X	X			X	X			X
							RA-5(5)	Vulnerability Scanning (Control Enhancement)			X	X			X	X			X	X			X
							RA-5(6)	Vulnerability Scanning (Control Enhancement)				X				X				X			
							RA-5(7)	Vulnerability Scanning (Control Enhancement)			X	X			X	X			X	X			X
							RA-5(8)	Vulnerability Scanning (Control Enhancement)				X				X				X			
							RA-5(9)	Vulnerability Scanning (Control Enhancement)				X				X				X			
							SA-10	Developer Configuration Management		X	X					X		X	X				
							SA-10(1)	Developer Configuration Management (Control Enhancement)								X							
							SA-10(2)	Developer Configuration Management (Control Enhancement)								X							
							SA-11	Developer Security Testing		X	X					X		X	X				
							SA-11(2)	Developer Security Testing (Control Enhancement)								X							
							SA-11(3)	Developer Security Testing (Control Enhancement)								X							
							SA-12	Supply Chain Protection			X					X		X	X				
							SA-12(1)	Supply Chain Protection (Control Enhancement)								X							
							SA-12(2)	Supply Chain Protection (Control Enhancement)								X		X	X				
							SA-12(3)	Supply Chain Protection (Control Enhancement)								X							
							SA-12(4)	Supply Chain Protection (Control Enhancement)								X							
							SA-12(5)	Supply Chain Protection (Control Enhancement)								X							
							SA-12(6)	Supply Chain Protection (Control Enhancement)								X							
							SA-12(7)	Supply Chain Protection (Control Enhancement)								X							
							SA-13	Trustworthiness			X					X			X				
							SA-14	Critical Information System Components								X		X	X				
							SA-14(1)	Critical Information System Components (Control Enhancement)								X		X	X				
							SA-3	Life Cycle Support	X	X	X					X	X	X	X				
							SA-4(1)	Acquisitions (Control Enhancement)		X	X					X		X	X				
							SA-4(2)	Acquisitions (Control Enhancement)			X					X			X				
							SA-4(4)	Acquisitions (Control Enhancement)		X	X					X							
							SA-4(5)	Acquisitions (Control Enhancement)								X							
							SA-5(1)	Information System Documentation (Control Enhancement)		X	X					X		X	X				
							SA-5(3)	Information System Documentation (Control Enhancement)		X	X					X		X	X				
							SA-5(4)	Information System Documentation (Control Enhancement)								X							
							SA-5(5)	Information System Documentation (Control Enhancement)								X							

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							SA-6(1)	Software Usage Restrictions (Control Enhancement)				X		X	X	X		X	X				
							SA-7	User Installed Software	X	X	X					X	X	X	X				
							SC-10	Network Disconnect		X	X	X		X	X	X		X	X				
							SC-11	Trusted Path								X							
							SC-12(1)	Cryptographic Key Establishment and Management (Control Enhancement)			X									X			X
							SC-13(4)	Use of Cryptography (Control Enhancement)								X							
							SC-15(1)	Collaborative Computing Devices (Control Enhancement)				X											
							SC-15(3)	Collaborative Computing Devices (Control Enhancement)				X				X							
							SC-16(1)	Transmission of Security Attributes (Control Enhancement)								X							
							SC-18(1)	Mobile Code (Control Enhancement)								X							
							SC-18(2)	Mobile Code (Control Enhancement)								X							
							SC-18(3)	Mobile Code (Control Enhancement)								X		X	X				
							SC-18(4)	Mobile Code (Control Enhancement)								X		X	X				
							SC-2(1)	Application Partitioning (Control Enhancement)				X				X							
							SC-20	Secure Name /Address Resolution Service (Authoritative Source)	X	X	X					X	X	X	X				
							SC-20(1)	Secure Name /Address Resolution Service (Authoritative Source) (Control Enhancement)	X	X	X					X	X	X	X				
							SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)			X					X			X				
							SC-21(1)	Secure Name /Address Resolution Service (Recursive or Caching Resolver) (Control Enhancement)								X							
							SC-22	Architecture and Provisioning for Name/Address Resolution Service		X	X	X		X	X	X		X	X	X		X	X
							SC-23	Session Authenticity		X	X					X		X	X				
							SC-23(1)	Session Authenticity (Control Enhancement)								X							
							SC-23(2)	Session Authenticity (Control Enhancement)								X							
							SC-23(3)	Session Authenticity (Control Enhancement)								X							
							SC-23(4)	Session Authenticity (Control Enhancement)								X							
							SC-24	Fail In Known State			X	X		X	X	X		X	X				
							SC-25	Thin Nodes								X							
							SC-26	Honeypots								X							
							SC-26(1)	Honeypots (Control Enhancement)								X							
							SC-27	Operating System-Independent Applications								X							
							SC-28(1)	Protection of Information at Rest (Control Enhancement)				X		X	X	X		X	X				
							SC-29	Heterogeneity								X							
							SC-3(1)	Security Function Isolation (Control Enhancement)				X				X							
							SC-3(2)	Security Function Isolation (Control Enhancement)				X				X							
							SC-3(3)	Security Function Isolation (Control Enhancement)				X				X							
							SC-3(4)	Security Function Isolation (Control Enhancement)				X				X							
							SC-3(5)	Security Function Isolation (Control Enhancement)				X				X							
							SC-30	Virtualization Techniques								X							
							SC-30(1)	Virtualization Techniques (Control Enhancement)								X							
							SC-30(2)	Virtualization Techniques (Control Enhancement)								X							
							SC-31	Covert Channel Analysis				X											
							SC-31(1)	Covert Channel Analysis (Control Enhancement)				X											

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A			
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							SC-32	Information System Partitioning		X	X	X		X	X	X		X	X				
							SC-33	Transmission Preparation Integrity								X							
							SC-34	Non-modifiable Executable Programs								X							
							SC-34(1)	Non-modifiable Executable Programs (Control Enhancement)								X							
							SC-34(2)	Non-modifiable Executable Programs (Control Enhancement)								X							
							SC-4(1)	Information In Shared Resources (Control Enhancement)				X											
							SC-5	Denial of Service Protection	X	X	X									X	X	X	X
							SC-5(1)	Denial of Service Protection (Control Enhancement)												X			
							SC-5(2)	Denial of Service Protection (Control Enhancement)												X			
							SC-6	Resource Priority												X			X
							SC-7(1)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(10)	Boundary Protection (Control Enhancement)				X											
							SC-7(11)	Boundary Protection (Control Enhancement)								X							
							SC-7(13)	Boundary Protection (Control Enhancement)				X				X							
							SC-7(14)	Boundary Protection (Control Enhancement)				X				X							
							SC-7(15)	Boundary Protection (Control Enhancement)				X				X							
							SC-7(16)	Boundary Protection (Control Enhancement)				X											
							SC-7(17)	Boundary Protection (Control Enhancement)								X							
							SC-7(18)	Boundary Protection (Control Enhancement)				X	X	X	X	X	X	X	X	X	X	X	X
							SC-7(2)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(3)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(4)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(5)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(6)	Boundary Protection (Control Enhancement)			X	X			X								
							SC-7(7)	Boundary Protection (Control Enhancement)		X	X	X		X	X	X		X	X				
							SC-7(8)	Boundary Protection (Control Enhancement)			X	X			X	X			X				
							SC-7(9)	Boundary Protection (Control Enhancement)				X				X							
							SC-8(1)	Transmission Integrity (Control Enhancement)		X	X					X		X	X				
							SC-8(2)	Transmission Integrity (Control Enhancement)								X		X	X				
							SC-9(2)	Transmission Confidentiality (Control Enhancement)				X											
							SI-10	Information Input Validation		X	X					X			X				
							SI-11	Error Handling		X	X					X			X				
							SI-13	Predictable Failure Prevention												X			
							SI-13(1)	Predictable Failure Prevention (Control Enhancement)												X			
							SI-13(2)	Predictable Failure Prevention (Control Enhancement)												X			
							SI-13(3)	Predictable Failure Prevention (Control Enhancement)												X			
							SI-13(4)	Predictable Failure Prevention (Control Enhancement)												X			
							SI-2(1)	Flaw Remediation (Control Enhancement)			X					X			X				
							SI-2(2)	Flaw Remediation (Control Enhancement)		X	X					X		X	X				
							SI-2(3)	Flaw Remediation (Control Enhancement)								X							
							SI-2(4)	Flaw Remediation (Control Enhancement)								X							

Appendix H – NIST SP 800-53r3 Security Controls With No Associations to DoDI 8500.2 Security Controls

DoDI 8500.2							NIST SP 800-53r3					CNSSI 1253													
CONTROL	MAC			CNF			CONTROL	CONTROL NAME	BSLN			C				I				A					
	I	II	III	CL	SN	PB			L	M	H	✓	L	M	H	✓	L	M	H	✓	L	M	H
							SI-3(1)	Malicious Code Protection (Control Enhancement)		X	X					X		X	X				
							SI-3(2)	Malicious Code Protection (Control Enhancement)		X	X					X		X	X				
							SI-3(3)	Malicious Code Protection (Control Enhancement)		X	X					X		X	X				
							SI-3(4)	Malicious Code Protection (Control Enhancement)								X							
							SI-3(5)	Malicious Code Protection (Control Enhancement)								X							
							SI-3(6)	Malicious Code Protection (Control Enhancement)								X							
							SI-4(1)	Information System Monitoring Tools and Techniques (Control Enhancement)								X							
							SI-4(11)	Information System Monitoring Tools and Techniques (Control Enhancement)				X											
							SI-4(12)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X							
							SI-4(13)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X				X			
							SI-4(14)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X							
							SI-4(15)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X							
							SI-4(16)	Information System Monitoring Tools and Techniques (Control Enhancement)								X							
							SI-4(17)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X							
							SI-4(2)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X					X		X	X				
							SI-4(3)	Information System Monitoring Tools and Techniques (Control Enhancement)								X							
							SI-4(4)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X	X			X	X		X	X				
							SI-4(5)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X					X		X	X				
							SI-4(6)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X					X		X	X				
							SI-4(7)	Information System Monitoring Tools and Techniques (Control Enhancement)								X				X			
							SI-4(8)	Information System Monitoring Tools and Techniques (Control Enhancement)				X				X				X			
							SI-4(9)	Information System Monitoring Tools and Techniques (Control Enhancement)								X							
							SI-5(1)	System Alerts, Advisories, and Directives (Control Enhancement)			X					X			X				
							SI-6(1)	Security Functionality Verification (Control Enhancement)								X							
							SI-6(2)	Security Functionality Verification (Control Enhancement)								X							
							SI-6(3)	Security Functionality Verification (Control Enhancement)								X							
							SI-7(1)	Software and Information Integrity (Control Enhancement)		X	X					X		X	X				
							SI-7(2)	Software and Information Integrity (Control Enhancement)			X					X			X				
							SI-7(3)	Software and Information Integrity (Control Enhancement)								X							
							SI-7(4)	Software and Information Integrity (Control Enhancement)								X							
							SI-8	Spam Protection		X	X					X	X	X	X	X	X	X	X
							SI-8(1)	Spam Protection (Control Enhancement)			X					X			X	X			X
							SI-8(2)	Spam Protection (Control Enhancement)								X				X			
							SI-9	Information Input Restrictions		X	X					X			X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
	Access Control																										
AC-1	Access Control Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					ECAN-1				C	C		4.B.1.a(1)(b)	1														
					ECPA-1	I	I	I																			
					PRAS-1					C																	
					PRAS-2				C																		
AC-2	Account Management				ECAN-1					C		4.B.2.a(3)	2			X	X	X	X	X	X	X	X				
					IAAC-1				C	C																	
AC-2(1)	Account Management (Control Enhancement)	X	X	X				C								X		X	X	X		X	X				
AC-2(2)	Account Management (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-2(3)	Account Management (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-2(4)	Account Management (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-2(5)	Account Management (Control Enhancement)															X				X							
AC-2(6)	Account Management (Control Enhancement)				ECAN-1				C	C						X				X							
AC-2(7)	Account Management (Control Enhancement)				ECPA-1	I	I	I								X			X	X			X				
AC-3	Access Enforcement	X	X	X	DCFA-1	I	I	I				4.B.2.a(2)	2			X	X X	X	X	X	X X	X	X				
					DCNR-1	I	I	I				4.B.4.a(3)	4														
					ECAN-1				C	C																	
					EBRU-1				C	C																	
					ECAN-1				C	C																	
					ECCD-1			I																			
					ECCD-2	I	I		I																		
					ECCR-2				C																		
					ECIC-1				C	C																	
					ECSD-2		I																				
					PRNK-1				C	C	C																
~~AC-3(1)~~	~~Access Enforcement (Control Enhancement)~~ *[Withdrawn: Incorporated into SC-10]*				[N/A] I																						
AC-3(2)	Access Enforcement (Control Enhancement)															X				X							
AC-3(3)	Access Enforcement (Control Enhancement)				ECAN-1				C	C						X				X							
AC-3(4)	Access Enforcement (Control Enhancement)				ECIC-1					C						X	X	X	X	X	X	X	X				
AC-3(5)	Access Enforcement (Control Enhancement)															X				X							
AC-3(6)	Access Enforcement (Control Enhancement)							C								X				X							
AC-4	Information Flow Enforcement		X	X	EBBD-1						C	4.B.3.a(3)	3			X		X	X	X		X	X				
					EBBD-2					C		7.B.3.g															
					EBBD-3				C																		
					EBCR-1	A	A	A																			
AC-4(1)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(2)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(3)	Information Flow Enforcement (Control Enhancement)															X				X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
AC-4(4)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(5)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(6)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(7)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(8)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(9)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(10)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(11)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(12)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(13)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(14)	Information Flow Enforcement (Control Enhancement)				ECIC-1				C	C						X				X							
AC-4(15)	Information Flow Enforcement (Control Enhancement)				ECIC-1				C	C						X				X							
AC-4(16)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-4(17)	Information Flow Enforcement (Control Enhancement)															X				X							
AC-5	Separation of Duties		X	X	ECLP-1				C	C	C	4.B.3.a(18)	3			X			X	X			X				
AC-6	Least Privilege		X	X	ECLP-1				C	C	C	4.B.2.a(10)	2			X	X	X	X	X	X	X	X				
AC-6(1)	Least Privilege (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-6(2)	Least Privilege (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-6(3)	Least Privilege (Control Enhancement)															X				X							
AC-6(4)	Least Privilege (Control Enhancement)															X				X							
AC-6(5)	Least Privilege (Control Enhancement)															X		X	X	X		X	X				
AC-6(6)	Least Privilege (Control Enhancement)															X				X							
AC-7	Unsuccessful Login Attempts	X	X	X	ECLO-1					C		4.B.2.a(17)(c)-(d)	2			X	X	X	X	X	X	X	X		X	X	X
					ECLO-2				C																		
AC-7(1)	Unsuccessful Login Attempts (Control Enhancement)															X		X	X	X		X	X				
AC-7(2)	Unsuccessful Login Attempts (Control Enhancement)															X											
AC-8	System Use Notification	X	X	X	ECWM-1				C	C	C	4.B.1.a(6)	1			X	X	X	X	X	X	X	X				
AC-9	Previous Logon (Access) Notification				ECLO-2				C											X		X	X				
AC-9(1)	Previous Logon (Access) Notification (Control Enhancement)																			X							
AC-9(2)	Previous Logon (Access) Notification (Control Enhancement)																			X							
AC-9(3)	Previous Logon (Access) Notification (Control Enhancement)																			X							
AC-10	Concurrent Session Control			X	ECLO-1					C		4.B.2.a(17)(a)	2							X		X	X				
					ECLO-2				C																		
AC-11	Session Lock		X	X	PESL-1	I	I	I				4.B.1.a(5)	1			X	X	X	X	X	X	X	X				
AC-11(1)	Session Lock (Control Enhancement)				PESL-1	I	I	I								X	X	X	X								
~~AC-12~~	~~Session Termination~~ *[Withdrawn: Incorporated into SC-10]*				[N/A]							4.B.2.a(17)(b)															
~~AC-12(1)~~	*[Withdrawn: Incorporated into SC-10]*				[N/A]																						

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
~~AC-13~~	~~Supervision and Review – Access Control~~ *[Withdrawn: Incorporated into AC-2 and AU-6]*				[N/A]							2.B.7.c 4.B.3.a(8)(b)															
~~AC-13(1)~~	*[Withdrawn: Incorporated into AC-2 and AU-6]*				[N/A]																						
AC-14	Permitted Actions without Identification or Authentication	X	X	X								7.D.3.a				X	X	X	X	X	X	X	X				
AC-14(1)	Permitted Actions without Identification or Authentication (Control Enhancement)		X	X												X		X	X	X		X	X				
~~AC-15~~	~~Automated Marking~~ *[Withdrawn: Incorporated into AC-16]*				[N/A]							4.B.2.a(11)															
AC-16	~~Automated Labeling~~ Security Attributes [Name Changed]				ECAD-1 ECML-1			C	C C	C C		4.B.1.a(3) 4.B.4.a(15) 4.B.4.a(16)	1 4 4			X	X	X	X	X	X	X	X				
AC-16(1)	Security Attributes (Control Enhancement)															X				X							
AC-16(2)	Security Attributes (Control Enhancement)																			X							
AC-16(3)	Security Attributes (Control Enhancement)																			X							
AC-16(4)	Security Attributes (Control Enhancement)															X	X	X	X	X	X	X	X				
AC-16(5)	Security Attributes (Control Enhancement)															X											
AC-17	Remote Access	X	X	X	EBRP-1 EBRU-1 ECCT-1				C C	C C C		4.B.1.a(1)(b) 4.B.3.a(11) 7.D.2.e	1 3			X	X	X	X	X	X	X	X				
AC-17(1)	Remote Access (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-17(2)	Remote Access (Control Enhancement)		X	X	EBRP-1 EBRU-1				C	C C						X	X	X	X	X	X	X	X				
AC-17(3)	Remote Access (Control Enhancement)		X	X				C								X		X	X	X		X	X				
AC-17(4)	Remote Access (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-17(5)	Remote Access (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-17(6)	Remote Access (Control Enhancement)		X	X												X		X	X								
AC-17(7)	Remote Access (Control Enhancement)			X	EBRP-1					C						X		X	X	X		X	X				
AC-17(8)	Remote Access (Control Enhancement)	X	X	X												X		X	X	X		X	X				
AC-18	Wireless Access Restrictions	X	X	X	ECCT-1 ECWN-1	A	A	C A		C		4.B.1.a(8) 5.B.3.a(11)	1	H		X	X	X	X	X	X	X	X				
AC-18(1)	Wireless Access Restrictions (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-18(2)	Wireless Access Restrictions (Control Enhancement)			X												X		X	X	X		X	X				
AC-18(3)	Wireless Access Restrictions (Control Enhancement)			X												X		X	X	X		X	X				
AC-18(4)	Wireless Access Restrictions (Control Enhancement)			X												X		X	X	X		X	X				
AC-18(5)	Wireless Access Restrictions (Control Enhancement)			X	ECTC-1					C						X		X	X	X		X	X				
AC-19	Access Control for ~~Portable and~~ Mobile Devices [*Name Modified*]	X	X	X	ECWN-1	A	A	A C				8.B.6.c 9.G.4				X	X	X	X	X	X	X	X				
AC-19(1)	Access Control for Mobile Devices (Control Enhancement)		X	X												X		X	X								
AC-19(2)	Access Control for Mobile Devices (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-19(3)	Access Control for Mobile Devices (Control Enhancement)		X	X												X		X	X	X		X	X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
AC-19(4)	Access Control for Mobile Devices (Control Enhancement)															X	X	X	X								
AC-20	Use of External Information Systems	X	X	X								8.B.6.c				X	X	X	X	X	X	X	X				
AC-20(1)	Use of External Information Systems (Control Enhancement)		X	X												X		X	X	X		X	X				
AC-20(2)	Use of External Information Systems (Control Enhancement)		X	X												X		X	X								
AC-21	User-Based Collaboration and Information Sharing [*New*]															X											
AC-21(1)	User-Based Collaboration and Information Sharing (Control Enhancement)															X											
AC-22	Publicly Accessible Content [*New*]	X	X	X												X	X	X	X								
Awareness and Training																											
AT-1	Security Awareness and Training Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.2.b(8)				X	X	X	X	X	X	X	X	X	X	X	X
					PRTN-1				I	I		2.B.4.e(6)															
AT-2	Security Awareness	X	X	X	PRTN-1				I	I		8.B.1				X	X	X	X	X	X	X	X	X	X	X	X
AT-2(1)	Security Awareness (Control Enhancement)															X				X				X			
AT-3	Security Training	X	X	X	PRTN-1				I	I		8.B.1				X	X	X	X	X	X	X	X	X	X	X	X
AT-3(1)	Security Training (Control Enhancement)																							X			
AT-3(2)	Security Training (Control Enhancement)															X			X	X			X	X			X
AT-4	Security Training Records	X	X	X								8.B.1				X	~~X~~	X	X	X	~~X~~	X	X	X	~~X~~	X	X
AT-5	Contacts with Security Groups and Associations															X				X				X			
Audit and Accountability																											
AU-1	Audit and Accountability Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					ECAT-1			I		I	I	4.B.2.a(4)	2														
					ECAT-2	I	I		I																		
					ECTB-1	I	I	I																			
AU-2	Auditable Events	X	X	X	ECAN-1					C		4.B.2.a(4)(d)	2			X	X	X	X	X	X	X	X				
					ECAR-1						C																
					ECAR-2			C		C																	
					ECAR-3				C																		
					ECCD-2	I	I		I																		
					ECND-2	I	I																				
~~AU-2(1)~~	~~Auditable Events (Control Enhancement)~~ *[Withdrawn Incorporated into AU-12]*				[N/A]																						
~~AU-2(2)~~	~~Auditable Events (Control Enhancement)~~ *[Withdrawn Incorporated into AU-12]*				[N/A]																						
AU-2(3)	Auditable Events (Control Enhancement)		X	X												X		X	X	X		X	X				
AU-2(4)	Auditable Events (Control Enhancement)		X	X												X	X	X	X	X	X	X	X				
AU-3	Content of Audit Records	X	X	X	ECAR-1						C	4.B.2.a(4)(a)	2			X	X	X	X	X	X	X	X				
					ECAR-2					C		4.B.2.a(5)(a)	2														
					ECAR-3				C																		
					ECLC-1				C																		
AU-3(1)	Content of Audit Records (Control Enhancement)		X	X												X		X	X	X		X	X				
AU-3(2)	Content of Audit Records (Control Enhancement)			X												X			X	X			X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
AU-4	Audit Storage Capacity	X	X	X								5.B.2.a(5)(a)(1)		M										X	X	X	X
AU-5	Response to Audit Processing Failures	X	X	X	ECAT-2	I	I		I			4.B.4.a(9)(d)	4											X	X	X	X
AU-5(1)	Response to Audit Processing Failures (Control Enhancement)			X																				X			X
AU-5(2)	Response to Audit Processing Failures (Control Enhancement)			X																				X			X
AU-5(3)	Response to Audit Processing Failures (Control Enhancement)																							X			
AU-5(4)	Response to Audit Processing Failures (Control Enhancement)															X				X							
AU-6	Audit ~~Monitoring~~ Review, Analysis, and Reporting [*Name Modified*]	X	X	X	ECAT-1			I		I	I	4.B.4.a(10)	4			X	X	X	X	X	X	X	X				
					ECAT-2	I	I		I																		
AU-6(1)	Audit Review, Analysis, and Reporting (Control Enhancement)			X												X			X	X			X				
~~AU-6(2)~~	~~Audit Review, Analysis, and Reporting (Control Enhancement)~~ *[Withdrawn; Incorporated into SI-4]*				[N/A]																						
AU-6(3)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-6(4)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-6(5)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-6(6)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-6(7)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-6(8)	Audit Review, Analysis, and Reporting (Control Enhancement)															X		X	X	X		X	X				
AU-6(9)	Audit Review, Analysis, and Reporting (Control Enhancement)															X				X							
AU-7	Audit Reduction and Report Generation		X	X	ECRG-1	I	I	I				4.B.3.a(6)	3			X		X	X	X		X	X				
AU-7(1)	Audit Reduction and Report Generation (Control Enhancement)		X	X												X		X	X	X		X	X				
AU-8	Time Stamps	X	X	X	ECAR-1						C	4.B.2.a(4)(a)	2							X	X	X	X				
					ECAR-2					C																	
					ECAR-3				C																		
					ECLC-1				C																		
AU-8(1)	Time Stamps (Control Enhancement)		X	X																X		X	X				
AU-9	Protection of Audit Information	X	X	X	ECTP-1		I	I				4.B.2.a(4)(b)	2			X	X	X	X	X	X	X	X				
AU-9(1)	Protection of Audit Information (Control Enhancement)																			X							
AU-9(2)	Protection of Audit Information (Control Enhancement)				ECTB-1	I	I	I																X			
AU-9(3)	Protection of Audit Information (Control Enhancement)																			X							
AU-9(4)	Protection of Audit Information (Control Enhancement)																			X							
AU-10	Non-repudiation			X								5.B.3.a(8)		H						X		X	X				
AU-10(1)	Non-repudiation (Control Enhancement)																			X							
AU-10(2)	Non-repudiation (Control Enhancement)																			X							
AU-10(3)	Non-repudiation (Control Enhancement)																			X							
AU-10(4)	Non-repudiation (Control Enhancement)																			X							
AU-10(5)	Non-repudiation (Control Enhancement)				DCNR-1	I	I	I												X		X	X				
AU-11	Audit Record Retention	X	X	X	ECRR-1				I	I	I	4.B.2.a(4)(c)	2											X	X	X	X
AU-12	Audit Generation [*New*]	X	X	X	ECAT-1			I		I	I					X	X	X	X	X	X	X	X	X	X	X	X
					ECAT-2	I	I		I																		
AU-12(1)	Audit Generation (Control Enhancement)			X																X			X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
AU-12(2)	Audit Generation (Control Enhancement)																			X							
AU-13	Monitoring For Information Disclosure [*New*]															X											
AU-14	Session Audit [*New*]																							X			
AU-14(1)	Session Audit (Control Enhancement)																							X			
Certification, Accreditation, and Security Assessments																											
CA-1	~~Certification, Accreditation, and Security Assessment Policies and Procedures~~ Security Assessment and Authorization Policies [Name Changed]	X	X	X	DCAR-1	A	A	A				2.B.2.b(1)				X	X	X	X	X	X	X	X	X	X	X	X
					DCII-1	I	I	I																			
CA-2	Security Assessments	X	X	X	DCAR-1	A	A	A				4.B.2.b(6)	2			X	X	X	X	X	X	X	X	X	X	X	X
					DCII-1	I	I	I				5.B.1.b(1)		B													
					PEPS-1				C	C		9.B.1															
												9.B.4															
CA-2(1)	Security Assessments (Control Enhancement)			X	DCAR-1	A	A	A								X			X	X			X	X			X
CA-2(2)	Security Assessments (Control Enhancement)	X		X	ECMT-1					C	C					X	X		X	X	X		X	X	X		X
					ECMT-2					C	C						X				X				X		
					PEPS-1				C	C																	
CA-3	Information System Connections	X	X	X	DCID-1	I	I	I				9.B.3				X	X	X	X	X	X	X	X				
					EBBD-1						C	9.D.3.c															
					EBBD-2					C																	
					EBBD-3				C																		
					EBCR-1	A	A	A																			
					EBRU-1				C	C																	
					EBPW-1					C	C																
					ECIC-1				C	C																	
CA-3(1)	Information System Connections (Control Enhancement)				EBBD-1						C					X											
					EBBD-2					C																	
CA-3(2)	Information System Connections (Control Enhancement)				EBBD-3				C							X	X	X	X								
~~CA-4~~	~~Security Certification~~ *[Withdrawn: Incorporated into CA-2]*				[N/A]							4.B.3.b(8)															
												9.E.2.a(2)															
												9.E.2.a(3)															
CA-5	Plan of Action and Milestones	X	X	X								9.E.2.a(3)(a)				X	X	X	X	X	X	X	X	X	X	X	X
CA-5(1)	Plan of Action and Milestones (Control Enhancement)															X				X				X			
CA-6	Security ~~Accreditation~~ Authorization [*Name Modified*]	X	X	X								9.D.3				X	X	X	X	X	X	X	X	X	X	X	X
												9.D.4															
CA-7	Continuous Monitoring	X	X	X	DCPR-1	I	I	I				2.B.4.e(7)				X	X	X	X	X	X	X	X	X	X	X	X
												2.B.5.c(10)															
												5.B.2.b(2)		M													
												9.B.1															
												9.D.7															
CA-7(1)	Continuous Monitoring (Control Enhancement)															X		X	X	X		X	X	X		X	X

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
CA-7(2)	Continuous Monitoring (Control Enhancement)				ECMT-1					C	C					X		X	X	X		X	X	X		X	X
					ECMT-2					C	C																
					VIVM-1	A	A	A																			
	Configuration Management																										
CM-1	Configuration Management Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X				
					DCPR-1	I	I	I				5.B.2.a(5)		M													
CM-2	Baseline Configuration	X	X	X	DCHW-1	A	A	A				2.B.7.c(7)								X	X	X	X				
					DCSW-1	A	A	A				4.B.1.c(3)	1														
					ECIM-1	I	I	I				4.B.2.b(6)	2														
CM-2(1)	Baseline Configuration (Control Enhancement)		X	X																X		X	X				
CM-2(2)	Baseline Configuration (Control Enhancement)			X																X			X				
CM-2(3)	Baseline Configuration (Control Enhancement)		X	X																X		X	X				
CM-2(4)	Baseline Configuration (Control Enhancement)		X																	X		X					
CM-2(5)	Baseline Configuration (Control Enhancement)			X																X			X				
CM-2(6)	Baseline Configuration (Control Enhancement)			X																X			X				
CM-3	Configuration Change Control		X	X	DCCB-1			I				2.B.7.c(7)								X		X	X				
					DCCB-2	I	I					4.B.1.c(3)	1														
					DCPR-1	I	I	I				4.B.2.b(6)	2														
					ECSD-2	I	I					5.B.2.a(5)		M													
CM-3(1)	Configuration Change Control (Control Enhancement)			X																X			X				
CM-3(2)	Configuration Change Control (Control Enhancement)			X	DCII-1	I	I	I														X	X				
CM-3(3)	Configuration Change Control (Control Enhancement)	X																	X	X							
CM-3(4)	Configuration Change Control (Control Enhancement)				DCCB-2	I	I															X	X				
CM-4	~~Monitoring Configuration Changes~~ Security Impact Analysis [Name Changed]	X	X	X	DCCT-1	I	I	I				2.B.7.c(7)							X			X	X				
					DCII-1	I	I	I				4.B.1.c(3)	1						X								
					DCPR-1	I	I	I				5.B.2.b(2)		M													
												8.B.8.c(7)															
CM-4(1)	Security Impact Analysis (Control Enhancement)			X	DCCT-1	I	I	I															X				
					DCSQ-1	I	I	I											X								
CM-4(2)	Security Impact Analysis (Control Enhancement)				DCCT-1	I	I	I												X							
CM-5	Access Restrictions for Change		X	X	DCPR-1	I	I	I				5.B.3.a(2)(b)		H								X	X				
					ECSD-1			I											X								
					ECSD-2	I	I																				
CM-5(1)	Access Restrictions for Change (Control Enhancement)			X																X		X	X				
CM-5(2)	Access Restrictions for Change (Control Enhancement)			X																X			X				
CM-5(3)	Access Restrictions for Change (Control Enhancement)			X																X			X				
CM-5(4)	Access Restrictions for Change (Control Enhancement)																			X							
CM-5(5)	Access Restrictions for Change (Control Enhancement)				DCSL-1	I	I	I												X							
					ECPC-1			I																			
					ECPC-2	I	I																				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
CM-5(6)	Access Restrictions for Change (Control Enhancement)																			X		X	X				
CM-5(7)	Access Restrictions for Change (Control Enhancement)																			X							
CM-6	Configuration Settings	X	X	X	DCSS-1			I				4.B.2.a(10)	2							X	X	X	X				
					DCCS-2	I	I																				
					DCPR-1	I	I	I																			
						A	A	A																			
CM-6(1)	Configuration Settings (Control Enhancement)			X																X			X				
CM-6(2)	Configuration Settings (Control Enhancement)			X	ECSC-1															X			X				
CM-6(3)	Configuration Settings (Control Enhancement)		X	X																X		X	X				
CM-6(4)	Configuration Settings (Control Enhancement)				DCCT-1	I	I	I												X							
CM-7	Least Functionality	X	X	X	ECIM-1	I	I	I				4.B.2.a(10)	2			X	X	X	X	X	X	X	X				
						A	A	A				7.D.2.b															
CM-7(1)	Least Functionality (Control Enhancement)		X	X	DCPP-1	A	A	A								X		X	X	X		X	X				
CM-7(2)	Least Functionality (Control Enhancement)			X	ECVI-1											X			X	X			X				
CM-7(3)	Least Functionality (Control Enhancement)															X		X	X	X		X	X				
CM-8	Information System Component Inventory	X	X	X	DCHW-1	A	A	A				2.B.7.c(7)								X	X	X	X				
						A	A	A				4.B.1.c(3)	1														
												4.B.2.b(6)	2														
CM-8(1)	Information System Component Inventory (Control Enhancement)		X	X	DCSW-1															X		X	X				
CM-8(2)	Information System Component Inventory (Control Enhancement)			X																X			X				
CM-8(3)	Information System Component Inventory (Control Enhancement)			X																X			X				
CM-8(4)	Information System Component Inventory (Control Enhancement)			X																X			X				
CM-8(5)	Information System Component Inventory (Control Enhancement)		X	X																X		X	X				
CM-8(6)	Information System Component Inventory (Control Enhancement)																			X							
CM-9	Configuration Management Plan [*New*]		X	X	DCPR-1	I	I	I												X		X	X				
CM-9(1)	Configuration Management Plan (Control Enhancement)																			X							
	Contingency Planning																										
CP-1	Contingency Planning Policy and Procedures	X	X	X	COBR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					COTR-1	A	A	A				6.B.1.a(1)			B												
					DCAR-1	A	A	A																			
CP-2	Contingency Plan	X	X	X	COEF-1			A				6.B.2.b(1)			M									X	X	X	X
					COEF-2	A	A																				
CP-2(1)	Contingency Plan (Control Enhancement)		X	X																				X		X	X
CP-2(2)	Contingency Plan (Control Enhancement)			X																				X			X
CP-2(3)	Contingency Plan (Control Enhancement)			X	CODP-1			A																X			X
CP-2(4)	Contingency Plan (Control Enhancement)				CODP-2		A																	X			X
CP-2(5)	Contingency Plan (Control Enhancement)				CODP-3	A																		X			X
CP-2(6)	Contingency Plan (Control Enhancement)																							X			
CP-3	Contingency Training	X	X	X	PRTN-1				I	I		8.B.1												X	X	X	X
CP-3(1)	Contingency Training (Control Enhancement)			X																				X			X

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
CP-3(2)	Contingency Training (Control Enhancement)																							X			
CP-4	Contingency Plan Testing and Exercises	X	X	X	COED-1		A	A				6.B.3.b(2)(b)			H									X	X	X	X
					COED-2	A																					
CP-4(1)	Contingency Plan Testing and Exercises (Control Enhancement)		X	X																				X		X	X
CP-4(2)	Contingency Plan Testing and Exercises (Control Enhancement)			X																				X			X
CP-4(3)	Contingency Plan Testing and Exercises (Control Enhancement)																							X			
CP-4(4)	Contingency Plan Testing and Exercises (Control Enhancement)			X																				X		X	X
~~CP-5~~	~~Contingency Plan Update~~ *[Withdrawn: Incorporated into CP-2]*				[N/A]							6.B.3.b(2)			H												
CP-6	Alternate Storage Site		X	X	COBR-1	A	A	A				6.B.2.a(2)			M									X		X	X
					CODB-2		A					6.B.3.a(2)(d)			H												
CP-6(1)	Alternate Storage Site (Control Enhancement)		X	X																				X		X	X
CP-6(2)	Alternate Storage Site (Control Enhancement)			X																				X			X
CP-6(3)	Alternate Storage Site (Control Enhancement)		X	X																				X		X	X
CP-7	Alternate Processing Site		X	X	COAS-1			A				6.B.3.a(2)(d)			H									X		X	X
					COAS-2	A	A																				
					COSP-1		A	A																			
					COSP-2	A																					
CP-7(1)	Alternate Processing Site (Control Enhancement)		X	X																				X		X	X
CP-7(2)	Alternate Processing Site (Control Enhancement)		X	X																				X		X	X
CP-7(3)	Alternate Processing Site (Control Enhancement)		X	X																				X		X	X
CP-7(4)	Alternate Processing Site (Control Enhancement)			X	COAS-2	A	A																	X		X	X
CP-7(5)	Alternate Processing Site (Control Enhancement)		X	X	COEB-1			A											X				X	X			X
					COEB-2	A	A										X				X				X		
CP-8	Telecommunications Services		X	X								6.B.2.a(4)			M	X				X				X		X	X
CP-8(1)	Telecommunications Services (Control Enhancement)		X	X																				X		X	X
CP-8(2)	Telecommunications Services (Control Enhancement)		X	X																				X		X	X
CP-8(3)	Telecommunications Services (Control Enhancement)			X																				X			X
CP-8(4)	Telecommunications Services (Control Enhancement)			X																				X			X
CP-9	Information System Backup	X	X	X	CODB-1			A				6.B.1.a(2)			B	X	X	X	X	X	X	X	X	X	X	X	X
					CODB-2		A																				
CP-9(1)	Information System Backup (Control Enhancement)		X	X																X		X	X	X		X	X
CP-9(2)	Information System Backup (Control Enhancement)			X																X			X	X			X
CP-9(3)	Information System Backup (Control Enhancement)			X	COSW-1	A	A	A																X			X
CP-9(4)	~~Information System Backup (Control Enhancement)~~ *[Withdrawn; Incorporated into CP-9]*				[N/A]																						
CP-9(5)	Information System Backup (Control Enhancement)																							X			
CP-9(6)	Information System Backup (Control Enhancement)				CODB-3	A																		X			
CP-10	Information System Recovery and Reconstitution	X	X	X	COTR-1	A	A	A				4.B.1.a(4)	1											X	X	X	X
					ECND-1			I				6.B.1.a(1)			B												
					ECND-2	I	I					6.B.2.a(3)(d)			M												

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
CP-10(1)	~~Information System Recovery and Reconstitution (Control Enhancement)~~ *[Withdrawn; Incorporated into CP-4]*				[N/A]																						
CP-10(2)	Information System Recovery and Reconstitution (Control Enhancement)			X	ECDC-1	I	I													X		X	X	X		X	X
CP-10(3)	Information System Recovery and Reconstitution (Control Enhancement)	X	X	X																				X		X	X
CP-10(4)	Information System Recovery and Reconstitution (Control Enhancement)			X																X			X	X			X
CP-10(5)	Information System Recovery and Reconstitution (Control Enhancement)																							X			
CP-10(6)	Information System Recovery and Reconstitution (Control Enhancement)																			X				X		X	X
Identification and Authentication																											
IA-1	Identification and Authentication Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X				
					IAIA-1					C																	
					IAIA-2				C																		
IA-2	User Identification and Authentication (Organizational Users)	X	X	X	EBRU-1					C		4.B.2.a(7)	2			X	X	X	X	X	X	X	X				
					IAIA-1					C																	
					IAIA-2			C	C																		
IA-2(1)	User Identification and Authentication (Organizational Users) (Control Enhancement)	X	X	X												X	X	X	X	X	X	X	X				
IA-2(2)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X												X		X	X	X		X	X				
IA-2(3)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X												X		X	X	X		X	X				
IA-2(4)	User Identification and Authentication (Organizational Users) (Control Enhancement)															X			X	X			X				
IA-2(5)	User Identification and Authentication (Organizational Users) (Control Enhancement)				IAGA-1					C						X		X	X	X		X	X				
IA-2(6)	User Identification and Authentication (Organizational Users) (Control Enhancement)							C																			
IA-2(7)	User Identification and Authentication (Organizational Users) (Control Enhancement)															X				X							
IA-2(8)	User Identification and Authentication (Organizational Users) (Control Enhancement)		X	X												X	X	X	X	X	X	X	X				
IA-2(9)	User Identification and Authentication (Organizational Users) (Control Enhancement)			X												X		X	X	X		X	X				
IA-3	Device Identification and Authentication		X	X								4.B.5.a(14)	5			X		X	X	X		X	X				
IA-3(1)	Device Identification and Authentication (Control Enhancement)															X				X							
IA-3(2)	Device Identification and Authentication (Control Enhancement)															X				X							
IA-3(3)	Device Identification and Authentication (Control Enhancement)															X				X							
IA-4	Identifier Management	X	X	X	IAGA-1				C	C		4.B.1.a(2)	1			X	X	X	X	X	X	X	X				
					IAIA-1					C																	
					IAIA-2				C																		
IA-4(1)	Identifier Management (Control Enhancement)															X				X							
IA-4(2)	Identifier Management (Control Enhancement)																			X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
IA-4(3)	Identifier Management (Control Enhancement)																			X							
IA-4(4)	Identifier Management (Control Enhancement)															X		X	X	X		X	X				
IA-4(5)	Identifier Management (Control Enhancement)															X				X							
IA-5	Authenticator Management	X	X	X	IAGA-1					C		4.B.2.a(7)	2			X	X	X	X	X	X	X	X				
					IAIA-1					C		4.B.3.a(11)	3														
					IAIA-2			C	C																		
					IAKM-1			I																			
					IAKM-2	I	I																				
					IAKM-3				I																		
					IATS-1			I																			
					IATS-2	I	I																				
IA-5(1)	Authenticator Management (Control Enhancement)	X	X	X	IAIA-1					C						X			X	X			X				
					IAIA-2				C								X				X						
IA-5(2)	Authenticator Management (Control Enhancement)		X	X																X		X	X				
IA-5(3)	Authenticator Management (Control Enhancement)				IAIA-1					C										X		X	X				
					IAIA-2				C																		
IA-5(4)	Authenticator Management (Control Enhancement)															X		X	X	X		X	X				
IA-5(5)	Authenticator Management (Control Enhancement)				IAIA-1					C						X				X							
					IAIA-2				C																		
IA-5(6)	Authenticator Management (Control Enhancement)				IAIA-1					C						X	X	X	X	X	X	X	X				
					IAIA-2				C																		
IA-5(7)	Authenticator Management (Control Enhancement)															X		X	X								
IA-5(8)	Authenticator Management (Control Enhancement)															X				X							
IA-6	Authenticator Feedback	X	X	X								4.B.2.a(7)(g)	2			X	X	X	X								
IA-7	Cryptographic Module Authentication	X	X	X												X	X	X	X	X	X	X	X				
IA-8	Identification and Authentication (Non-Organizational Users) [*New*]	X	X	X												X	X	X	X	X	X	X	X				
Incident Response																											
IR-1	Incident Response Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-1		A	A				2.B.2.b(6)															
					VIIR-2	A						2.B.6.c(10)															
												8.B.7															
IR-2	Incident Response Training	X	X	X	PRTN-1				I	I		8.B.1.b(1)(f)				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-1		A	A				8.B.1.c(1)(e)															
					VIIR-2	A						8.B.1.c(2)(c)															
IR-2(1)	Incident Response Training (Control Enhancement)			X												X			X	X			X	X			X
IR-2(2)	Incident Response Training (Control Enhancement)			X												X			X	X			X	X			X
IR-3	Incident Response Testing and Exercises		X	X	VIIR-1		A	A				8.B.7				X			X	X			X	X			X
					VIIR-2	A											X				X				X		
IR-3(1)	Incident Response Testing and Exercises (Control Enhancement)			X												X			X	X			X	X			X
IR-4	Incident Handling	X	X	X	VIIR-1		A	A				8.B.7				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-2	A						9.B.2.e															

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
IR-4(1)	Incident Handling (Control Enhancement)		X	X												X			X	X			X	X			X
IR-4(2)	Incident Handling (Control Enhancement)															X	X			X	X			X	X		
IR-4(3)	Incident Handling (Control Enhancement)															X				X				X			
IR-4(4)	Incident Handling (Control Enhancement)															X				X				X			
IR-4(5)	Incident Handling (Control Enhancement)				ECAT-2	I	I		I							X				X							
IR-5	Incident Monitoring	X	X	X	VIIR-1		A	A				8.B.7.a				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-2	A																					
IR-5(1)	Incident Monitoring (Control Enhancement)			X												X			X	X			X	X			X
IR-6	Incident Reporting	X	X	X	VIIR-1		A	A				8.B.7				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-2	A																					
IR-6(1)	Incident Reporting (Control Enhancement)		X	X												X			X	X			X	X			X
IR-6(2)	Incident Reporting (Control Enhancement)															X	X			X	X			X	X		
IR-7	Incident Response Assistance	X	X	X	VIIR-1			A				8.B.7.c				X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-2	A A																					
IR-7(1)	Incident Response Assistance (Control Enhancement)		X	X												X			X	X			X	X			X
IR-7(2)	Incident Response Assistance (Control Enhancement)															X	X			X	X			X	X		
IR-8	Incident Response Plan [*New*]	X	X	X	VIIR-1			A								X	X	X	X	X	X	X	X	X	X	X	X
					VIIR-2	A A																					
Maintenance																											
MA-1	System Maintenance Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					PRMP-1					C	C	6.B.2.a(5)			M												
					PRMP-2				C																		
MA-2	Controlled Maintenance	X	X	X	PECS-1					C		6.B.2.a(5)			M	X	X	X	X	X	X	X	X	X	X	X	X
					PECS-2				C			8.B.8.c															
MA-2(1)	Controlled Maintenance (Control Enhancement)		X	X												X			X	X			X	X			X
MA-2(2)	Controlled Maintenance (Control Enhancement)			X												X	X		X	X	X		X	X	X		X
MA-3	Maintenance Tools		X	X								6.B.3.a(5)			H					X	X	X	X	X	X	X	X
												8.B.8.c(4)															
												8.B.8.c(5)															
MA-3(1)	Maintenance Tools (Control Enhancement)		X	X																X		X	X	X		X	X
MA-3(2)	Maintenance Tools (Control Enhancement)		X	X																X		X	X	X		X	X
MA-3(3)	Maintenance Tools (Control Enhancement)			X												X	X	X	X								
MA-3(4)	Maintenance Tools (Control Enhancement)																			X							
MA-4	~~Remote Maintenance~~ Non-Local Maintenance [Name Changed]	X	X	X	EBRP-1					C		8.B.8.d								X	X	X	X				
MA-4(1)	Non-Local Maintenance (Control Enhancement)			X	EBRP-1					C										X		X	X				
MA-4(2)	Non-Local Maintenance (Control Enhancement)	X	X	X				C												X		X	X				
MA-4(3)	Non-Local Maintenance (Control Enhancement)			X				C								X			X	X			X	X			
MA-4(4)	Non-Local Maintenance (Control Enhancement)															X				X							
MA-4(5)	Non-Local Maintenance (Control Enhancement)																			X							
MA-4(6)	Non-Local Maintenance (Control Enhancement)				EBRP-1				C	C						X				X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
MA-4(7)	Non-Local Maintenance (Control Enhancement)																			X							
MA-5	Maintenance Personnel	X	X	X	PRMP-1					C	C	8.B.8.a				X	X	X	X	X	X	X	X	X	X	X	X
					PRMP-2				C																		
MA-5(1)	Maintenance Personnel (Control Enhancement)				PRMP-2				C							X	X	X	X	X	X	X	X	X	X	X	X
MA-5(2)	Maintenance Personnel (Control Enhancement)				PRMP-2				C							X	X	X	X	X	X	X	X	X	X	X	X
MA-5(3)	Maintenance Personnel (Control Enhancement)				PRMP-2				C							X				X				X			
MA-5(4)	Maintenance Personnel (Control Enhancement)															X	X	X	X	X	X	X	X	X	X	X	X
MA-6	Timely Maintenance		X	X	COMS-1			A				6.B.2.a(5)			M									X		X	X
					COMS-2	A	A																				
							A	A																			
					COSP-2	A																					
	Media Protection																										
MP-1	Media Protection Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.6.c(7)				X	X	X	X	X	X	X	X	X	X	X	X
					PESP-1				C	C		8.B.2															
MP-2	Media Access	X	X	X	PEDI-1				I	I		2.B.9.b(4)				X	X	X	X								
					PEPF-1					C		4.B.1.a(1)	1														
					PEPF-2				C			4.B.1.a(7)	1														
MP-2(1)	Media Access (Control Enhancement)		X	X												X		X	X	X		X	X				
MP-2(2)	Media Access (Control Enhancement)															X				X							
MP-3	Media ~~Labeling~~ Marking [*Name Modified*]		X	X	ECML-1				C	C		2.B.9.b(4)				X	X	X	X								
												8.B.2.a															
												8.B.2.c															
MP-4	Media Storage		X	X	ECCR-1					C		2.B.9.b(4)				X	X	X	X								
					ECCR-2				C			4.B.1.a(7)	1														
					ECCR-3				C																		
					PESS-1				C	C																	
MP-4(1)	Media Storage (Control Enhancement)															X	X	X	X								
MP-5	Media Transport		X	X								2.B.9.b(4)				X		X	X	X		X	X				
~~MP-5(1)~~	~~Media Transport (Control Enhancement)~~ *[Withdrawn; Incorporated into MP-5]*				[N/A]																						
MP-5(2)	Media Transport (Control Enhancement)		X	X												X		X	X	X		X	X				
MP-5(3)	Media Transport (Control Enhancement)			X												X			X	X			X				
MP-5(4)	Media Transport (Control Enhancement)		X	X												X		X	X	X		X	X				
MP-6	Media Sanitization and Disposal [Name Modified]	X	X	X	PECS-1					C		8.B.5				X	X	X	X								
					PECS-2				C			2.B.9.b(4)															
					PEDD-1				C			8.B.5.a(4)															
												8.B.5.d															
												8.B.5.e															
MP-6(1)	Media Sanitization (Control Enhancement)			X												X			X								
MP-6(2)	Media Sanitization (Control Enhancement)			X												X			X								
MP-6(3)	Media Sanitization (Control Enhancement)			X												X			X								

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
MP-6(4)	Media Sanitization (Control Enhancement)				PECS-1					C						X											
MP-6(5)	Media Sanitization (Control Enhancement)				PECS-2				C							X	X	X	X								
MP-6(6)	Media Sanitization (Control Enhancement)				PEDD-1				C							X	X	X	X								
	Physical and Environmental Protection																										
PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					PETN-1	A	A	A				8.D															
PE-2	Physical Access Authorizations	X	X	X	PECF-1					C		4.B.1.a(1)	1			X	X	X	X	X	X	X	X	X	X	X	X
					PECF-2				C			8.E															
PE-2(1)	Physical Access Authorizations (Control Enhancement)															X				X				X			
PE-2(2)	Physical Access Authorizations (Control Enhancement)				PEPF-2				C							X				X							
PE-2(3)	Physical Access Authorizations (Control Enhancement)				PECF-2				C							X	X	X	X								
PE-3	Physical Access Control	X	X	X	PEPF-1					C		4.B.1.a(1)	1			X	X	X	X	X	X	X	X	X	X	X	X
					PEPF-2				C			8.D-2															
												8.E															
PE-3(1)	Physical Access Control (Control Enhancement)			X												X			X	X			X				
PE-3(2)	Physical Access Control (Control Enhancement)															X	X	X	X								
PE-3(3)	Physical Access Control (Control Enhancement)				PEPF-2				C							X	X	X	X	X	X	X	X				
PE-3(4)	Physical Access Control (Control Enhancement)															X				X							
PE-3(5)	Physical Access Control (Control Enhancement)																			X							
PE-3(6)	Physical Access Control (Control Enhancement)				PEPS-1				C	C										X			X				
PE-4	Access Control for Transmission Medium		X	X								8.D.2				X		X	X	X		X	X				
												4.B.1.a(8)	1														
PE-5	Access Control for ~~Display Medium~~ Output Devices [*Name Modified*]		X	X	PEDI-1					I		8.C.2.a				X		X	X								
					PEPF-1					C		8.D.2															
					PEPF-2			I	C																		
PE-6	Monitoring Physical Access	X	X	X	PEPF-2				C			4.B.1.a(1)	1			X	X	X	X	X	X	X	X	X	X	X	X
												8.C.2.a															
												8.D.2															
PE-6(1)	Monitoring Physical Access (Control Enhancement)		X	X	PEPF-2				C															X		X	X
PE-6(2)	Monitoring Physical Access (Control Enhancement)			X												X			X	X			X	X			X
PE-7	Visitor Control	X	X	X	PEVC-1				C	C		8.C.2.a				X	X	X	X	X	X	X	X				
												8.D.2															
												8.E															
PE-7(1)	Visitor Control (Control Enhancement)		X	X												X		X	X	X		X	X				
PE-7(2)	Visitor Control (Control Enhancement)															X				X							
PE-8	Access Records	X	X	X	PEPF-2				C			8.C.2.a				X	X	X	X	X	X	X	X				
					PEVC-1				C	C		8.D.2															
												8.E															
PE-8(1)	Access Records (Control Enhancement)			X																				X			X
PE-8(2)	Access Records (Control Enhancement)			X																				X			X

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
PE-9	Power Equipment and Power Cabling		X	X								8.D.2												X		X	X
PE-9(1)	Power Equipment and Power Cabling (Control Enhancement)																							X			
PE-9(2)	Power Equipment and Power Cabling (Control Enhancement)				PEVR-1	A	A	A																X		X	X
PE-10	Emergency Shutoff		X	X	PEMS-1	A	A	A				8.D.2												X		X	X
~~PE-10(1)~~	~~Emergency Shutoff (Control Enhancement)~~ *[Withdrawn; Incorporated into PE-10]*				[N/A]																						
PE-11	Emergency Power		X	X								6.B.2.a(6)			M									X		X	X
												6.B.2.a(7)			M												
PE-11(1)	Emergency Power (Control Enhancement)			X	COPS-1			A																X		X	
					COPS-2		A																				
					COPS-3	A																					
PE-11(2)	Emergency Power (Control Enhancement)				COPS-1			A																X			X
					COPS-2		A																				
					COPS-3	A																					
PE-12	Emergency Lighting	X	X	X	PEEL-1			A				8.D.2												X	X	X	X
					PEEL-2	A	A																				
PE-12(1)	Emergency Lighting (Control Enhancement)				PEEL-2	A	A																	X		X	X
PE-13	Fire Protection	X	X	X	PEFD-1			A				8.C.2.a												X	X	X	X
					PEFD-2	A	A					8.D.2															
					PEFI-1	A	A	A																			
					PEFS-1			A																			
					PEFS-2	A	A																				
PE-13(1)	Fire Protection (Control Enhancement)		X	X	PEFD-2	A	A																	X		X	X
PE-13(2)	Fire Protection (Control Enhancement)		X	X	PEFD-2	A	A																	X		X	X
					PEFS-2	A	A																				
PE-13(3)	Fire Protection (Control Enhancement)		X	X	PEFS-2	A	A																	X		X	X
PE-13(4)	Fire Protection (Control Enhancement)				PEFI-1	A	A	A																X		X	X
PE-14	Temperature and Humidity Controls	X	X	X	PEHC-1			A				8.D.2												X	X	X	X
					PEHC-2	A	A																				
					PETC-1			A																			
					PETC-2	A	A																				
PE-14(1)	Temperature and Humidity Controls (Control Enhancement)				PEHC-2	A	A																	X		X	X
					PETC-2	A	A																				
PE-14(2)	Temperature and Humidity Controls (Control Enhancement)				PEHC-1			A																X		X	X
					PETC-1			A																			
PE-15	Water Damage Protection	X	X	X								8.C.2.a												X	X	X	X
												8.D.2															
PE-15(1)	Water Damage Protection (Control Enhancement)			X																				X			X
PE-16	Delivery and Removal	X	X	X								8.B.5.e				X	X	X	X					X	X	X	X
PE-17	Alternate Work Site		X	X	EBRU-1				C	C						X			X	X			X	X			X
PE-18	Location of Information System Components		X	X													X				X			X	X	X	X

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
PE-18(1)	Location of Information System Components (Control Enhancement)			X																				X			X
PE-19	Information Leakage				ECTC-1					C						X		X	X			X	X				
PE-19(1)	Information Leakage (Control Enhancement)															X		X	X			X	X				
Planning																											
PL-1	Security Planning Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
PL-2	System Security Plan	X	X	X	DCSD-1	A	A	A				2.B.6.c(3) 2.B.7.c(5) 9.E.2.a(1)(d) 9.F.2.a				X	X	X	X	X	X	X	X	X	X	X	X
PL-2(1)	System Security Plan (Control Enhancement)				DCFA-1	I	I	I								X			X	X			X	X			X
PL-2(2)	System Security Plan (Control Enhancement)															X	X		X	X	X		X	X	X		X
~~PL-3~~	~~System Security Plan Update~~ [*Withdrawn: Incorporated into PL-2*]				[N/A]							2.B.7.c(5)					X				X				X		
PL-4	Rules of Behavior	X	X	X	PRRB-1	A	A	A				2.B.9.b				X	X	X	X	X	X	X	X	X	X	X	X
PL-4(1)	Rules of Behavior (Control Enhancement)															X											
PL-5	Privacy Impact Assessment	X	X	X								8.B.9				X	X	X	X								
PL-6	Security-Related Activity Planning		X	X												X			X	X			X	X			X
Personnel Security																											
PS-1	Personnel Security Policy and Procedures	X	X	X	DCAR-1 PRRB-1	A A	A A	A A				2.B.4.e(5) 8.E				X	X	X	X	X	X	X	X	X	X	X	X
PS-2	Position Categorization	X	X	X								8.E				X	X	X	X	X	X	X	X	X	X	X	X
PS-3	Personnel Screening	X	X	X	PRAS-1 PRAS-2				C	C		2.B.7.c(2) 2.B.8.b(5) 8.E				X	X	X	X	X	X	X	X				
PS-3(1)	Personnel Screening (Control Enhancement)															X	X	X	X								
PS-3(2)	Personnel Screening (Control Enhancement)															X	X	X	X								
PS-4	Personnel Termination	X	X	X	IAAC-1				C	C		2.B.9.b(6) 4.B.2.a(3)(e) 8.E	2			X	X	X	X	X	X	X	X	X	X	X	X
PS-5	Personnel Transfer	X	X	X	IAAC-1				C	C		2.B.9.b(6)				X	X	X	X	X	X	X	X	X	X	X	X
PS-6	Access Agreements	X	X	X	PRAS-1 PRAS-2 PRNK-1 PRRB-1	A	A	A	C C	C C	C	8.E				X	X	X	X	X	X	X	X				
PS-6(1)	Access Agreements (Control Enhancement)				PRAS-1 PRNK-1				C	C C	C					X	X		X	X	X		X				
PS-6(2)	Access Agreements (Control Enhancement)				PRAS-2 PRNK-1				C C	C	C					X	X	X	X								
PS-7	Third-Party Personnel Security	X	X	X	DCIT-1	I	I	I				8.D 8.E				X	X	X	X	X	X	X	X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
PS-8	Personnel Sanctions	X	X	X	PRRB-1	A	A	A				4.B.2.a(3)(e)	2			X	X	X	X	X	X	X	X	X	X	X	X
												8.E															
	Risk Assessment																										
RA-1	Risk Assessment Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
RA-2	Security Categorization	X	X	X								3.C				X	X	X	X	X	X	X	X	X	X	X	X
												3.D															
												9.E.2.a(1)(a)															
												9.E.2.a(1)(d)															
RA-3	Risk Assessment	X	X	X	DCAR-1	A	A	A				9.B				X	X	X	X	X	X	X	X	X	X	X	X
					DCDS-1	I	I	I																			
					DCII-1	I	I	I																			
~~RA-4~~	~~Risk Assessment Update~~ [*Withdrawn: Incorporated into RA-3*]				[N/A]							9.B.4.f															
												9.D.1.d															
RA-5	Vulnerability Scanning	X	X	X	ECMT-1					C	C	4.B.3.a(8)(b)	3			X	X	X	X	X	X	X	X	X	X	X	X
					ECMT-2					C	C	4.B.3.b(6)(b)	3														
						A	A	A				9.B.4.e															
RA-5(1)	Vulnerability Scanning (Control Enhancement)		X	X												X			X	X			X	X			X
RA-5(2)	Vulnerability Scanning (Control Enhancement)			X	VIVM-1											X	X		X	X	X		X	X	X		X
RA-5(3)	Vulnerability Scanning (Control Enhancement)			X												X	X		X	X	X		X	X	X		X
RA-5(4)	Vulnerability Scanning (Control Enhancement)			X												X			X	X			X	X			X
RA-5(5)	Vulnerability Scanning (Control Enhancement)			X												X			X	X			X	X			X
RA-5(6)	Vulnerability Scanning (Control Enhancement)															X				X				X			
RA-5(7)	Vulnerability Scanning (Control Enhancement)			X												X			X	X			X	X			X
RA-5(8)	Vulnerability Scanning (Control Enhancement)															X				X				X			
RA-5(9)	Vulnerability Scanning (Control Enhancement)															X				X				X			
	System and Services Acquisition																										
SA-1	System and Services Acquisition Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X				
SA-2	Allocation of Resources	X	X	X	DCPB-1	A	A					2.B.4.e(8)								X	X	X	X				
SA-3	Life Cycle Support	X	X	X								9.E.2								X	X	X	X				
SA-4	Acquisitions	X	X	X	DCDS-1	I	I	I				9.B.4								X	X	X	X				
					DCIT-1	I	I	I																			
					DCMC-1	I	I	I																			
					DCSR-1						C																
					DCSR-2					C																	
					DCSR-3				C																		
SA-4(1)	Acquisitions (Control Enhancement)		X	X																X		X	X				
SA-4(2)	Acquisitions (Control Enhancement)			X																X			X				
SA-4(3)	Acquisitions (Control Enhancement)				DCBP-1	I	I	I														X	X				
					DCSQ-1	I	I	I											X								
SA-4(4)	Acquisitions (Control Enhancement)		X	X																X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SA-4(5)	Acquisitions (Control Enhancement)																			X							
SA-4(6)	Acquisitions (Control Enhancement)				DCAS-1				C	C	C									X		X	X				
SA-4(7)	Acquisitions (Control Enhancement)				DCAS-1				C	C	C									X		X	X				
SA-5	Information System Documentation	X	X	X	DCCS-1			I				4.B.2.b(2)	2							X	X	X	X				
					DCCS-2	I	I					4.B.2.b(3)	2														
					DCFA-1	I	I	I				4.B.4.b(4)	4														
					DCHW-1	A	A	A				9.C.3															
					DCSD-1	A	A	A																			
					DCSW-1	A	A	A																			
					ECND-1			I																			
					ECND-2	I	I																				
SA-5(1)	Information System Documentation (Control Enhancement)		X	X																X		X	X				
SA-5(2)	Information System Documentation (Control Enhancement)			X	DCID-1	I	I	I															X				
SA-5(3)	Information System Documentation (Control Enhancement)		X	X															X	X		X	X				
SA-5(4)	Information System Documentation (Control Enhancement)																			X							
SA-5(5)	Information System Documentation (Control Enhancement)																			X							
SA-6	Software Usage Restrictions	X	X	X	DCPD-1	A	A	A				2.B.9.b(11)				X	X	X	X	X	X	X	X				
SA-6(1)	Software Usage Restrictions (Control Enhancement)															X		X	X	X		X	X				
SA-7	User Installed Software	X	X	X								2.B.9.b(11)									X	X	X				
SA-8	Security Engineering Principles		X	X	DCBP-1	I	I	I											X			X	X				
					DCCS-1			I											X								
					DCCS-2	I	I																				
SA-9	External Information System Services	X	X	X	DCDS-1	I	I	I				8.C.2								X	X	X	X				
					DCFA-1	I	I	I				8.E															
						I	I	I																			
						I	I	I																			
				DCID-1		A	A	A																			
SA-9(1)	External Information System Services (Control Enhancement)			DCIT-1	DCDS-1	I	I	I														X	X				
SA-10	Developer Configuration Management		X	X	DCPP-1							4.B.4.b(4)	4						X	X		X	X				
												8.C.2.a															
SA-10(1)	Developer Configuration Management (Control Enhancement)																			X							
SA-10(2)	Developer Configuration Management (Control Enhancement)																			X							
SA-11	Developer Security Testing		X	X								4.B.4.b(4)	4							X		X	X				
SA-11(1)	Developer Security Testing (Control Enhancement)				DCSQ-1	I	I	I												X							
SA-11(2)	Developer Security Testing (Control Enhancement)																			X							
SA-11(3)	Developer Security Testing (Control Enhancement)																			X							
SA-12	Supply Chain Protection [*New*]			X																X		X	X				
SA-12(1)	Supply Chain Protection (Control Enhancement)																			X							
SA-12(2)	Supply Chain Protection (Control Enhancement)																			X		X	X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SA-12(3)	Supply Chain Protection (Control Enhancement)																			X							
SA-12(4)	Supply Chain Protection (Control Enhancement)																			X							
SA-12(5)	Supply Chain Protection (Control Enhancement)																			X							
SA-12(6)	Supply Chain Protection (Control Enhancement)																			X							
SA-12(7)	Supply Chain Protection (Control Enhancement)																			X							
SA-13	Trustworthiness [*New*]			X																X			X				
SA-14	Critical Information System Components [*New*]																			X		X	X				
SA-14(1)	Critical Information System Components (Control Enhancement)																			X		X	X				
	System and Communications Protection																										
SC-1	System and Communications Protection Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
					ECCM-1				C																		
SC-2	Application Partitioning		X	X	DCPA-1	I	I	I				4.B.3.b(6)(a)	3			X			X	X			X				
												4.B.4.b(8)	4				X				X						
												5.B.3.b(2)		H													
SC-2(1)	Application Partitioning (Control Enhancement)															X				X							
SC-3	Security Function Isolation			X	DCSP-1	I	I					4.B.3.b(6)(a)	3			X		X	X	X		X	X				
												4.B.4.b(8)	4														
												5.B.3.b(1)		H													
												5.B.3.b(2)		H													
SC-3(1)	Security Function Isolation (Control Enhancement)															X				X							
SC-3(2)	Security Function Isolation (Control Enhancement)															X				X							
SC-3(3)	Security Function Isolation (Control Enhancement)															X				X							
SC-3(4)	Security Function Isolation (Control Enhancement)															X				X							
SC-3(5)	Security Function Isolation (Control Enhancement)															X				X							
SC-4	Information ~~Remnance~~ In Shared Resources [*Name Modified*]		X	X	ECRC-1					C		4.B.2.a(14)	2			X		X	X								
SC-4(1)	Information In Shared Resources (Control Enhancement)															X											
SC-5	Denial of Service Protection	X	X	X				C				6.B.3.a(6)			H									X	X	X	X
SC-5(1)	Denial of Service Protection (Control Enhancement)																							X			
SC-5(2)	Denial of Service Protection (Control Enhancement)																							X			
SC-6	Resource Priority											6.B.3.a(11)			H									X			X
SC-7	Boundary Protection	X	X	X	COEB-1			A				4.B.4.a(27)	4			X	X	X	X	X	X	X	X				
					COEB-2	A	A					5.B.3.a(11)(b)		H													
					EBBD-1						C	7.A.3															
					EBBD-2					C		7.B															
					EBBD-3				C			7.C															
					EBCR-1	A	A	A				7.D															
					EBPW-1					C	C																
					EBRU-1				C	C																	
					ECIM-1	I	I	I																			
					ECVI-1	A	A	A																			

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SC-7(1)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(2)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(3)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(4)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(5)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(6)	Boundary Protection (Control Enhancement)			X												X			X								
SC-7(7)	Boundary Protection (Control Enhancement)		X	X												X		X	X	X		X	X				
SC-7(8)	Boundary Protection (Control Enhancement)			X												X			X	X			X				
SC-7(9)	Boundary Protection (Control Enhancement)															X				X							
SC-7(10)	Boundary Protection (Control Enhancement)															X											
SC-7(11)	Boundary Protection (Control Enhancement)																			X							
SC-7(12)	Boundary Protection (Control Enhancement)				ECID-1	I	I									X			X	X			X				X
SC-7(13)	Boundary Protection (Control Enhancement)															X	X			X	X				X		
SC-7(14)	Boundary Protection (Control Enhancement)															X				X							
SC-7(15)	Boundary Protection (Control Enhancement)															X				X							
SC-7(16)	Boundary Protection (Control Enhancement)															X											
SC-7(17)	Boundary Protection (Control Enhancement)																			X							
SC-7(18)	Boundary Protection (Control Enhancement)															X	X	X	X	X	X	X	X	X	X	X	X
SC-8	Transmission Integrity		X	X	ECCM-1				C			5.B.3.a(11)		H						X	X	X	X				
					ECTM-1			I																			
					ECTM-2	I	I																				
SC-8(1)	Transmission Integrity (Control Enhancement)		X	X																X		X	X				
SC-8(2)	Transmission Integrity (Control Enhancement)																			X		X	X				
SC-9	Transmission Confidentiality		X	X	ECCM-1				C			4.B.1.a(8)(a)	1			X	X	X	X								
SC-9(1)	Transmission Confidentiality (Control Enhancement)		X	X	ECCT-1					C						X	X	X	X								
					ECCT-2				C																		
					ECNK-1				C	C																	
					ECNK-2				C																		
SC-9(2)	Transmission Confidentiality (Control Enhancement)															X											
SC-10	Network Disconnect		X	X								4.B.2.a(17)	2			X		X	X	X		X	X				
SC-11	Trusted Path											4.B.4.a(14)	4							X							
SC-12	Cryptographic Key Establishment and Management	X	X	X	IAKM-1											X	X	X	X	X	X	X	X				
					IAKM-2	I	I																				
					IAKM-3		I		I																		
SC-12(1)	Cryptographic Key Establishment and Management (Control Enhancement)			X																				X			X
SC-12(2)	Cryptographic Key Establishment and Management (Control Enhancement)				IAKM-1			I								X				X							
SC-12(3)	Cryptographic Key Establishment and Management (Control Enhancement)				IAKM-2	I	I									X				X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
					IAKM-3				I																		
SC-12(4)	Cryptographic Key Establishment and Management (Control Enhancement)				IAKM-1			I								X				X							
					IATS-1			I																			
SC-12(5)	Cryptographic Key Establishment and Management (Control Enhancement)				IAKM-2	I	I									X				X							
					IATS-1			I																			
					IATS-2	I	I																				
SC-13	Use of Cryptography	X	X	X	IAKM-1			I								X	X	X	X	X	X	X	X				
					IAKM-2	I	I																				
					IAKM-3				I																		
					IATS-1			I																			
					IATS-2	I	I																				
SC-13(1)	Use of Cryptography (Control Enhancement)				ECCR-1					C						X											
					IAKM-1			I																			
					IAKM-2	I	I																				
SC-13(2)	Use of Cryptography (Control Enhancement)				ECCR-3				C							X	X	X	X								
					IAKM-2	I	I																				
					IAKM-3				I																		
SC-13(3)	Use of Cryptography (Control Enhancement)				ECCR-2				C							X											
SC-13(4)	Use of Cryptography (Control Enhancement)																			X							
SC-14	Public Access Protections	X	X	X	EBPW-1					C	C									X	X	X	X	X	X	X	X
SC-15	Collaborative Computing Devices [*Name Modified*]	X	X	X	ECVI-1	A	A	A				7.G				X	X	X	X								
SC-15(1)	Collaborative Computing Devices (Control Enhancement)															X											
SC-15(2)	Collaborative Computing Devices (Control Enhancement)				ECIM-1	I	I	I								X			X	X			X				
SC-15(3)	Collaborative Computing Devices (Control Enhancement)															X	X			X	X						
SC-16	Transmission of Security ~~Parameters~~ Attributes [*Name Modified*]				ECTM-2	I	I					4.B.1.a(3)	1			X		X	X	X		X	X				
SC-16(1)	Transmission of Security Attributes (Control Enhancement)																			X							
SC-17	Public Key Infrastructure Certificates		X	X	IAKM-1			I				2.B.4.e(5)				X			X	X			X				
					IAKM-2	I	I					4.B.3.a(11)	3				X				X						
					IAKM-3				I																		
SC-18	Mobile Code		X	X	DCMC-1	I	I	I				2.B.4.e(5)								X	X	X	X				
												7.E															
SC-18(1)	Mobile Code (Control Enhancement)																			X							
SC-18(2)	Mobile Code (Control Enhancement)																			X							
SC-18(3)	Mobile Code (Control Enhancement)																			X		X	X				
SC-18(4)	Mobile Code (Control Enhancement)																			X		X	X				
SC-19	Voice Over Internet Protocol		X	X	ECVI-1	A	A	A								X		X	X	X		X	X				
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	X	X	X																X	X	X	X				
SC-20(1)	Secure Name /Address Resolution Service (Authoritative Source) (Control Enhancement)	X	X	X																X	X	X	X				

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)			X																X			X				
SC-21(1)	Secure Name /Address Resolution Service (Recursive or Caching Resolver) (Control Enhancement)																			X							
SC-22	Architecture and Provisioning for Name/Address Resolution Service		X	X												X		X	X	X		X	X	X		X	X
SC-23	Session Authenticity		X	X																X		X	X				
SC-23(1)	Session Authenticity (Control Enhancement)																			X							
SC-23(2)	Session Authenticity (Control Enhancement)																			X							
SC-23(3)	Session Authenticity (Control Enhancement)																			X							
SC-23(4)	Session Authenticity (Control Enhancement)																			X							
SC-24	Fail In Known State [*New*]			X												X		X	X	X		X	X				
SC-25	Thin Nodes [*New*]																			X							
SC-26	Honeypots [*New*]																			X							
SC-26(1)	Honeypots (Control Enhancement)																			X							
SC-27	Operating System-Independent Applications [*New*]																			X							
SC-28	Protection of Information at Rest [*New*]		X	X	ECCR-1					C						X			X	X			X				
					ECCR-2				C								X				X						
					ECCR-3				C																		
SC-28(1)	Protection of Information at Rest (Control Enhancement)															X		X	X	X		X	X				
SC-29	Heterogeneity [*New*]																			X							
SC-30	Virtualization Techniques [*New*]																			X							
SC-30(1)	Virtualization Techniques (Control Enhancement)																			X							
SC-30(2)	Virtualization Techniques (Control Enhancement)																			X							
SC-31	Covert Channel Analysis [*New*]															X											
SC-31(1)	Covert Channel Analysis (Control Enhancement)															X											
SC-32	Information System Partitioning [*New*]		X	X												X		X	X	X		X	X				
SC-33	Transmission Preparation Integrity [*New*]																			X							
SC-34	Non-modifiable Executable Programs [*New*]																			X							
SC-34(1)	Non-modifiable Executable Programs (Control Enhancement)																			X							
SC-34(2)	Non-modifiable Executable Programs (Control Enhancement)																			X							
System and Information Integrity																											
SI-1	System and Information Integrity Policy and Procedures	X	X	X	DCAR-1	A	A	A				2.B.4.e(5)				X	X	X	X	X	X	X	X	X	X	X	X
												5.B.1.b(1)		B													
												5.B.2.a(5)(a)(1)		M													
SI-2	Flaw Remediation	X	X	X	DCCT-1	I	I	I				5.B.2.a(5)(a)(3)		M							X	X	X				
					DCSQ-1	I	I	I				6.B.2.a(5)			M				X								
					VIVM-1	A	A	A																			
SI-2(1)	Flaw Remediation (Control Enhancement)			X																X			X				
SI-2(2)	Flaw Remediation (Control Enhancement)		X	X																X		X	X				
SI-2(3)	Flaw Remediation (Control Enhancement)																			X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SI-2(4)	Flaw Remediation (Control Enhancement)																			X							
SI-3	Malicious Code Protection	X	X	X	ECVP-1	A	A	A				5.B.1.a(4)		B						X	X	X	X				
					VIVM-1	A	A	A				7.B.4.b(1)															
SI-3(1)	Malicious Code Protection (Control Enhancement)		X	X																X		X	X				
SI-3(2)	Malicious Code Protection (Control Enhancement)		X	X																X		X	X				
SI-3(3)	Malicious Code Protection (Control Enhancement)		X	X																X		X	X				
SI-3(4)	Malicious Code Protection (Control Enhancement)																			X							
SI-3(5)	Malicious Code Protection (Control Enhancement)																			X							
SI-3(6)	Malicious Code Protection (Control Enhancement)																			X							
SI-4	Information System Monitoring Tools and Techniques		X	X	EBBD-1						C	4.B.2.a(5)(b)	2							X		X	X				
					EBBD-2					C		4.B.3.a(8)(b)	3														
					EBBD-3				C			6.B.3.a(8)			H												
					ECID-1	I	I																				
SI-4(1)	Information System Monitoring Tools and Techniques (Control Enhancement)																			X							
SI-4(2)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X																X		X	X				
SI-4(3)	Information System Monitoring Tools and Techniques (Control Enhancement)																			X							
SI-4(4)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X												X			X	X		X	X				
SI-4(5)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X																X		X	X				
SI-4(6)	Information System Monitoring Tools and Techniques (Control Enhancement)		X	X																X		X	X				
SI-4(7)	Information System Monitoring Tools and Techniques (Control Enhancement)																			X				X			
SI-4(8)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X				X			
SI-4(9)	Information System Monitoring Tools and Techniques (Control Enhancement)																			X							
SI-4(10)	Information System Monitoring Tools and Techniques (Control Enhancement)				EBVC-1	A	A	A								X			X	X			X				
SI-4(11)	Information System Monitoring Tools and Techniques (Control Enhancement)															X	X				X						
SI-4(12)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X							
SI-4(13)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X				X			
SI-4(14)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X							

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2						DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
SI-4(15)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X							
SI-4(16)	Information System Monitoring Tools and Techniques (Control Enhancement)																			X							
SI-4(17)	Information System Monitoring Tools and Techniques (Control Enhancement)															X				X							
SI-5	Security Alerts, ~~and~~ Advisories, and Directives [*Name Modified*]	X	X	X	VIVM-1	A	A	A				8.B.7									X	X	X				
SI-5(1)	System Alerts, Advisories, and Directives (Control Enhancement)			X															X	X			X				
SI-6	Security Functionality Verification			X	DCSS-1			I				4.B.1.c(2)	1							X		X	X				
					DCSS-2	I	I		I			5.B.2.b(2)		M													
SI-6(1)	Security Functionality Verification (Control Enhancement)																			X							
SI-6(2)	Security Functionality Verification (Control Enhancement)																			X							
SI-6(3)	Security Functionality Verification (Control Enhancement)																			X							
SI-7	Software and Information Integrity		X	X	ECSD-2	I	I					4.B.1.c(2)	1									X	X				
					ECTM-1			I				5.B.1.a(3)		B					X								
					ECTM-2	I	I					5.B.2.a(6)		M													
SI-7(1)	Software and Information Integrity (Control Enhancement)		X	X																X		X	X				
SI-7(2)	Software and Information Integrity (Control Enhancement)			X																X			X				
SI-7(3)	Software and Information Integrity (Control Enhancement)																			X							
SI-7(4)	Software and Information Integrity (Control Enhancement)																			X							
SI-8	Spam Protection		X	X								5.B.1.a(4)		B						X	X	X	X	X	X	X	X
SI-8(1)	Spam Protection (Control Enhancement)			X																X			X	X			X
SI-8(2)	Spam Protection (Control Enhancement)																			X				X			
SI-9	Information Input Restrictions		X	X								2.B.9.b(11)								X			X				
SI-10	~~Information Accuracy, Completeness, Validity, and Authenticity~~ Information Input Validation [Name Changed]		X	X								7.B.2.h								X			X				
												2.B.4.d															
SI-11	Error Handling		X	X								2.B.4.d								X			X				
SI-12	Information Output Handling and Retention	X	X	X	PESP-1					C		2.B.4.d				X	X	X	X	X	X	X	X				
												8.B.9															
								C				8.G															
SI-13	Predictable Failure Prevention [*New*]																							X			
SI-13(1)	Predictable Failure Prevention (Control Enhancement)																							X			
SI-13(2)	Predictable Failure Prevention (Control Enhancement)																							X			
SI-13(3)	Predictable Failure Prevention (Control Enhancement)																							X			
SI-13(4)	Predictable Failure Prevention (Control Enhancement)																							X			
Information Security Program Plan																											
PM-1	Information Security Program Plan	X	X	X												X				X				X			
PM-2	Senior Information Security Officer	X	X	X												X				X				X			
PM-3	Information Security Resources	X	X	X												X				X				X			

Appendix I – NIST SP 800-53r3 Security Control Mapping

NIST SP 800-53r3					DoDI 8500.2							DCID 6/3				CNSSI 1253											
CONTROL	CONTROL NAME	BSLN			CONTROL	MAC			CNF			CONTROL	C	I	A	C				I				A			
		L	M	H		I	II	III	CL	SN	PB		PL	LOC	LOC	✓	L	M	H	✓	L	M	H	✓	L	M	H
PM-4	Plan of Action and Milestones Process	X	X	X												X				X				X			
PM-5	Information System Inventory	X	X	X												X				X				X			
PM-6	Information Security Measures of Performance	X	X	X												X				X				X			
PM-7	Enterprise Architecture	X	X	X	DCFA-1	I	I	I								X											
PM-8	Critical Infrastructure Plan	X	X	X												X			X	X			X	X			
PM-9	Risk Management Strategy	X	X	X												X				X				X			
PM-10	Security Authorization Process	X	X	X												X				X				X			
PM-11	Mission/Business Process Definition	X	X	X												X				X				X			