



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

September 28, 2005

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
ATTN: CHIEF INFORMATION OFFICER
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
ATTN: CHIEF INFORMATION OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ATTN: CHIEF INFORMATION OFFICER
DIRECTOR, ADMINISTRATION AND MANAGEMENT
ATTN: CHIEF INFORMATION OFFICER
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
OSD CHIEF INFORMATION OFFICER
DIRECTORS OF THE DEFENSE AGENCIES
ATTN: CHIEF INFORMATION OFFICER
DIRECTORS OF THE FIELD ACTIVITIES
ATTN: CHIEF INFORMATION OFFICER**

**SUBJECT: Department of Defense (DoD) Information Technology (IT) Registry Merger
Into the DoD IT Portfolio Repository (DITPR)**

This memorandum provides guidance for executing the task to begin merging the DoD IT Registry into DITPR by October 31, 2005, contained in the Deputy Chief Information Officer memorandum of June 15, 2005, "Department of Defense (DoD) Information Technology Portfolio Repository (DITPR)."

The current DoD IT Registry is used as the official DoD data source to meet a number of external and internal requirements including:

- The DoD-wide inventory of mission critical (MC) and mission essential (ME) systems required by 10 USC 2223(a)(5). In addition to the Title 10 requirements, the DoD IT Registry is the repository for Mission Support (MS) systems (those that are neither MC nor ME).
- Compilation of the reports required by the Federal Information Security Management Act (FISMA) of 2002.
- Compilation of the Privacy Impact Assessment compliance information in accordance with OMB Memorandum, September 26, 2003, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," II.C.3.a.ii.

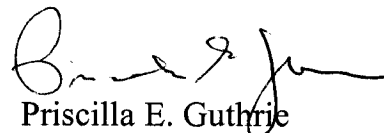
- Compilation of the E-Authentication Report, in accordance with OMB memorandum M-04-04, December 16, 2003, "E-Authentication Guidance for Federal Agencies."
- Official registry for systems in accordance with DoDI 5000.2, May 12, 2003, "Operation of the Defense Acquisition System," Enclosure E.4.2.4.1.

With the completion of the merger of the DoD IT Registry into DITPR as outlined in this document, DITPR will become the official unclassified DoD data source for FISMA, E-Authentication, Portfolio Management, Privacy Impact Assessments, the inventory of MC/ME/MS systems, and the registry for systems under DODI 5000.2.

Our goal is to further progress towards implementation of the DoD Net-Centric Data Strategy and achieving a net-centric environment to eliminate duplicative and overlapping data calls and consolidate guidance. Towards that end, an IT Management Data Community of Interest (COI) will be formed. Further details will be provided separately.

CIOs from the Military Departments, Combatant Commands, Joint Staff, Defense Agencies, Defense Field Activities, and the OSD CIO will identify a point of contact for the merger by October 1, 2005, and, as necessary, register users for DITPR accounts no later than October 31, 2005. Component points of contact shall participate in a meeting on Wednesday, October 12, 2005, in Crystal Mall 3, Suite 600 Conference Room, from 1000-1200, where the merger guidance will be reviewed in detail.

For additional information about the merger, contact Mr. Kevin Garrison, (703) 602-0980, Ext 149, DSN 332, kevin.garrison.ctr@osd.mil or Mr. Les Bloom, (703) 602-0980, Ext 133, DSN 332, leslie.bloom@osd.mil.



Priscilla E. Guthrie
Deputy Assistant Secretary of Defense
(Deputy CIO)

Attachments:

Appendix A – Merger Process Overview

Appendix B – Common Data Elements

Appendix C – DoD IT Registry Data Elements for Merger

Appendix D – DITPR Data Elements to be Completed for Systems Added from the DoD IT Registry

Appendix E – Detailed Instructions & Milestones

cc:

Under Secretaries of Defense

Assistant Secretaries of Defense

General Counsel of the Department of Defense

Director, Operational Test and Evaluation

Assistants to the Secretary Of Defense

Director, Program Analysis and Evaluation

Director, Net Assessment

Director, Force Transformation

Transformation Support Office

Appendix A – Merger Process Overview

The merger of the DoD IT Registry into DITPR will be conducted as follows:

1. Normal DITPR operations will not be affected by the merger. Components will be able to continue to make changes in DITPR before, during, and after the merger period. If DITPR operations preclude a start date of October 31, 2005, the merger plan and time line will be revised.
2. Systems in the SIPRNET version of the DoD IT Registry will not be moved to DITPR. The SIPRNET version of the DoD IT Registry will continue to operate until an alternative is developed and approved.
3. Previously issued policy guidance for the DoD IT Registry, FISMA, E-Authentication, and DITPR remains in effect with the following modifications:
 - a. DCIO Memorandum, December 21, 2004, “Department of Defense (DoD) Information Technology (IT) Registry Guidance for Fiscal Year 2005 (FY05)”:
 - (1) Mission Support systems will be added as follows:
 - (a) 50% by December 1, 2005 into the DoD IT Registry
 - (b) 75% by March 1, 2006 into DITPR (or SIPRNET version of the DoD IT Registry)
 - (c) 100% by September 30, 2006 into DITPR (or SIPRNET version of the DoD IT Registry)
 - (2) Quarterly updates will be as follows:
 - (a) December 1, 2005 in the IT Registry
 - (b) March 1, June 1, and September 1 in DITPR or the SIPRNET DoD IT Registry
 - b. CIO Memorandum, April 14, 2005, “Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2005 (FY05)”:
 - (1) Enclaves and outsourced IT-based processes that have a separate C&A must be in the DoD IT Registry. After December 16, 2005 they must be in DITPR or the SIPRNET version of the DoD IT Registry.
 - (2) All systems in DITPR must be updated with FISMA data by 16 December 2005.
 - c. DCIO Memorandum, March 24, 2005, “Supplemental Guidance for the E-Authentication Fields Within the Department of Defense (DoD) Information Technology (IT) Registry”:

Appendix A – Merger Process Overview

- (1) All DoD Component CIOs will ensure all systems meeting the E-Authentication reporting criteria are entered into the DoD IT Registry and all E-Authentication data elements populated by December 1, 2005.
4. On October 31, 2005, existing data on systems in the DoD IT Registry will be automatically loaded into DITPR as follows:
 - a. Systems not already in DITPR will be added automatically.
 - b. Systems already in DITPR will be handled as follows:
 - (1) If selected common data elements between the two system entries match, the system will be automatically added to DITPR.
 - (2) If selected common data elements between the two system entries do not match, the system will move to a Component Holding Area. Components will have 30 days to resolve the differences. At the end of the 30-day resolution period, the system will be automatically added to DITPR with the common data from the current official DoD data source (the DoD IT Registry) overwriting the entries in DITPR.
 - c. Systems in DITPR but not in the DoD IT Registry will not be affected but will be required to comply with the data element population due dates contained herein.
 - d. Criteria to be used to determine existence of a record match in both the DoD IT Registry and DITPR, as well as how common data elements will be matched are in Appendix E.
5. The DoD IT Registry will continue to be used as the official DoD data source until the end of the merger period (January 31, 2006). Components will conduct the quarterly update (to include the addition of at least 50% of Mission Support systems) not later than December 1, 2005 in the DoD IT Registry.
6. The DoD Quarterly FISMA Report for December 2005 and the DoD E-Authentication Report will use the DoD IT Registry as the official data source.
7. On December 16, 2005, systems in the DoD IT Registry will be automatically loaded into DITPR using the same method described above. Upon completion of the load from the DoD IT Registry into DITPR, the DoD IT Registry will be locked and Components will not be able to make any changes to data in the DoD IT Registry.

Appendix A – Merger Process Overview

8. Between December 16, 2005 and January 31, 2006 Components will resolve data for systems in the Component Holding Area. On January 31, 2006, the Component Holding Area will be shut down.

9. On January 31, 2006, DITPR will become the official unclassified DoD data source for FISMA, E-Authentication, Privacy Impact Assessment, MC/ME/MS systems inventory, and registry for DoDI 5000.2 IT systems.

10. On February 1, 2006 the unclassified DoD IT Registry will be archived and operations discontinued. Between December 16, 2005 and January 31, 2006, there will be a backup plan for continued operations of the DoD IT Registry in case of major system problems in DITPR.

11. During the period between October 31 and December 16, Components making changes to systems data must ensure that the entries in the DoD IT Registry and DITPR are synchronized and consistent.

12. To preclude multiple conflicting adjustments to the number of systems in DITPR, the current Domain Database holding area will be archived effective October 1, 2005 and retained until January 31, 2006.

13. Further details, milestones, and coordinating instructions are at Appendix E.

Appendix B – Common Data Elements

The following data elements are common to both the DoD IT Registry and DITPR. The right hand column in the table below depicts what the field length will be when implemented in DITPR at the start of the merger.

Field	Current IT Registry	Current DITPR	Merger Implementation
System Name	100	200	DITPR (200)
System Description	1000	200	1000
System Acronym	30	50	DITPR (50)
Component	From List	From List	See Appendix C
Life Cycle	List	List	See Appendix C
ACAT	List	List	See Appendix C
DODREGID	Components create	Components Enter	Retain (archived)
BIN	6	20	4

Notes:

- DODREGID will be editable by Components in DITPR until 31 Jan 05, at which time it will be archived (changed to not editable by Components) and retained for crosswalk purposes and audits.

Appendix C –IT Registry Data Elements for Merger

The current DoD IT Registry data dictionary will be adjusted as part of the merger into DITPR. There are three categories of changes:

1. Data elements that will be added or changed during the merger.
2. Data elements that will not change during the merger.
3. Data elements that will be eliminated during the merger.

The following data elements will be added to or changed in the DoD IT Registry and DITPR:

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
Modified List	COMPONENT	25	Executive Agency or DoD Component that owns this entry and is forwarding the data file to the data repository. For acceptable values, see Table 1.	Component Name, See Table 1	Mandatory for all entries	Core System Info
New	SUB_COMPONENT	50 Text	Optional entry. Provides capability to indicate which element within the Component provides information about or manages the system.	Text	Optional	Other System Info
Field Size Change	SYSTEM_ACRONYM	50	A shortened or commonly used name or abbreviation (upper case) for this entry.	Text	Mandatory for all entries	Core System Info
Field Size Change	SYSTEM_NAME	200	The full descriptive name for this entry (upper case).	Text	Mandatory for all entries	Core System Info
Modified List	ACAT	3	Acquisition Category (from DODI 5000.2), Table E2.T1 (Description and Decision Authority for ACAT I-III Programs). ACAT I MDAP (10 USC 2430, reference (n)) ; Dollar value: estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than \$365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than \$2.190 billion in FY 2000 constant dollars. ACAT ID: USD(AT&L); ACAT IC: Head of the DoD Component or, if delegated, the DoD Component Acquisition Executive (CAE)	IC, ID, IAM, IAC, II, III, NA	Mandatory for all entries	Core System Info

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>ACAT IA MAIS: Dollar value of AIS estimated by the DoD Component Head to require program costs (all appropriations) in any single year in excess of \$32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of \$126 million in FY 2000 constant dollars, or total life-cycle costs in excess of \$378 million in FY 2000 constant dollars. MDA designation as special interest: ACAT IAM: ASD(C3I)/DoD CIO; ACAT IAC: CAE, as delegated by the DoD CIO</p> <p>ACAT II (Does not meet criteria for ACAT I) Major system. Dollar value: estimated by the DoD Component Head to require an eventual total expenditure for RDT&E of more than \$140 million in FY 2000 constant dollars, or for procurement of more than \$660 million in FY 2000 constant dollars (10 USC 2302d, reference (o))</p> <p>ACAT III (Does not meet criteria for ACAT II or above) Less-than a MAIS program; designated by the DoD CAE at the lowest level appropriate</p>			
Field Size Change	PM_NAME_LAST	30	Last name of Program Manager (PM) or POC for this entry	Last Name	Mandatory for all entries	Core System Info
New	PM_NAME_FIRST	30	First name of Program Manager (PM) or POC for this entry	First Name	Mandatory for all entries	Core System Info
Field Size Change	PM_TITLE	8	Rank, Grade, and Title of PM or POC or Systems Manager.	Rank or Grade and Title	Mandatory for all entries	Core System Info
Field Size	PM_COM_PHONE	25	Commercial phone number of PM or POC or Systems Manager.	Phone number with	Mandatory for all	Core

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
Change				extension	entries	System Info
Field Size Change	PM_DSN_PHONE	15	Defense Switched Network phone number of PM or POC or Systems Manager.	Phone number with extension	Mandatory for all entries	Core System Info
Field Size Change	PM_EMAIL	50	Email address of PM or POC or Systems Manager.	E-mail	Mandatory for all entries	Core System Info
Field Size Change	DAA_NAME_LAST	30	Designated Approving Authority (DAA) Information: Last name of the DAA who granted the system a certification and accreditation (C&A) status.	Last name	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
New	DAA_NAME_FIRST	30	Designated Approving Authority (DAA) Information: First name of the DAA who granted the system a certification and accreditation (C&A) status.	First name	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
Field Size Change	DAA_TITLE	8	Designated Approving Authority (DAA) Information: Title of the DAA who granted the system a certification and accreditation (C&A) status.	Title	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
Field Size Change	DAA_PHONE	25	Designated Approving Authority (DAA) Information: Phone number of the DAA who granted the system a certification and accreditation (C&A) status.	Phone Number and Extension	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
New	DAA_DSN_PHONE	15	Defense Switched Network phone number of DAA who granted the system a certification and accreditation (C&A) status.	Phone Number and Extension	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
Field Size Change	DAA_EMAIL	50	Designated Approving Authority (DAA) Information: Electronic mail address of the DAA who granted the system a certification and accreditation (C&A) status.	E-mail address	Mandatory for all entries that answer “Yes” to	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
					ACCRED-RQD	
Modified Field Name, Description, and List	IA_REC_TYPE	64	<p>Information Assurance Record Type:</p> <ul style="list-style-type: none"> • Automated Information System Application (8500.2) <ul style="list-style-type: none"> – For DoD IA purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DoD Directive 5000.1. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). • Enclave (8500.2) <ul style="list-style-type: none"> – Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. • Outsourced IT-based Process (8500.2) <ul style="list-style-type: none"> – General term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. 	<p>AIS Application</p> <p>Enclave</p> <p>Outsourced IT-based Process</p> <p>Platform IT Interconnection</p> <p>Not an IA Record Type</p>	Mandatory for all entries	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<ul style="list-style-type: none"> • Platform IT Interconnection (8500.2) <ul style="list-style-type: none"> – For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration • Not an IA Record Type (derived from 8500.1 and 8500.2) <ul style="list-style-type: none"> – The entry is not a DoD information system. DODD 8500.1: “For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.” 			
Field Length Changed	BIN	4	Insert the Initiative Number if it exists, from the Select and Native Application Program-Information Technology (SNaP-IT) Database.	Numerical Entry	Mandatory for all Defense Business Systems	Other System Info
Modified List	LIFE_CYCLE	64	Life Cycle Definition – What phase of the system life cycle is this IT Registry entity in? (DoDI 5000.2 and Attachment A “IRB Guidance for Completing the Appendix E Certification Template” to	Concept Refinement Technology	Mandatory for all entries	Core System Info

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>USD(AT&L) Memorandum, “Release of the DoD Business Systems Investment Review Proposal Submission Guideline for the Investment Review Process” July 18, 2005)</p> <ul style="list-style-type: none"> • Concept Refinement • Technology Development • System Development & Demonstration • Production & Deployment • Operations & Support <p>Not defined in DoDI 5000.2 but in Appendix E cited above:</p> <ul style="list-style-type: none"> • Modernization/Enhancement: A stage in a systems life where it is gaining functionality • Migration: Any point in a systems life where it is losing functionality • Archive: A point in a systems life cycle where it is running solely to maintain archived information (usually for legal reasons) • Browning Out/Retirement: The stage of a systems life when it is shutdown and all of its functionality has been migrated or determined as obsolete and killed 	<p>Development</p> <p>System Development & Demonstration</p> <p>Production & Deployment</p> <p>Operations & Support</p> <p>Operations & Support – Modernization/ Enhancement</p> <p>Operations & Support – Migration</p> <p>Operations & Support – Brown Out/ Retirement</p> <p>Archive</p>		
Privacy Impact Assessments: 3 new data elements and changes to field names and descriptions.						
New	IDENTIFIABLE_INFO	3	Identifiable Information. Identifies whether system contains Federally-owned information in an identifiable form as defined in OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIA; which states:	Yes, No	Mandatory for all entries/E-Gov Act 2002	PIA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>“<i>Information in identifiable form</i> - is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).²</p> <p>²Information in identifiable form is defined in section 208(d) of the Act as “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” Information “permitting the physical or online contacting of a specific individual”</p> <p>For further guidance, see paragraph II.A: http://www.whitehouse.gov/omb/memoranda/m03-22.html</p>			
New Name & Description	PIA_RQD	3	<p>PIA Required. Identifies whether a privacy impact assessment is required for a new or previously existing IT system based on the provisions in OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIB; which states:</p> <p>B. <i>When to conduct a PIA:</i>⁵</p> <ol style="list-style-type: none"> 1. <i>The E-Government Act requires agencies to conduct a PIA before:</i> <ol style="list-style-type: none"> a. developing or procuring IT systems or projects that collect, maintain or disseminate information in 	Yes, No	Mandatory for all entries/E-Gov Act 2002	PIA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>identifiable form from or about members of the public (excluding DoD personnel), or</p> <p>b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). Excluding DoD personnel</p> <p>2. <i>In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks” (for a listing of “system changes” see OMB Memo, attachment A, paragraph II.B.2.a-i)</i></p> <p>http://www.whitehouse.gov/omb/memoranda/m03-22.html</p> <p>For a listing of under what conditions a PIA is not required, see paragraph II.B.3.a-g.</p> <p>⁵ In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).</p>			
Modified	PIA_RVW	3	<p>PIA Reviewed. Identifies whether the PIA has been reviewed (by the Component Privacy Office and CIO) and approved in accordance with OMB Memorandum 2002, dated September 26, 2003, Attachment A, paragraph IIC3ai.</p> <p>http://www.whitehouse.gov/omb/memoranda/m03-22.html</p> <p>Indicate "Not Applicable" only if a PIA is not required. If "No" is indicated, provide explanation.</p>	Yes, No, NA	Mandatory for all entries for which PIA is required	PIA
New Field	PIA_PUBLIC_AVAIL	3	PIA Public Availability. Identifies whether the PIA has been made	Yes, No, NA	Mandatory for all	PIA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
Name			<p>available for public review in accordance with OMB Memorandum "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, Attachment A, paragraph IIC3aiii. www.whitehouse.gov/omb/memoranda/m03-22.html</p> <p>Indicate "Not Applicable" only if a PIA is not required. If "No" is indicated, provide explanation.</p>		entries for which a PIA is required	
New Field Name	PIA_SUBMIT_OMB	3	<p>PIA Submission to OMB. Identifies whether a copy of the PIA has been provided to OMB in accordance with OMB Circular NO. A-11, "Preparation, Submission, and Execution of the Budget", 2005, which states:</p> <p>"Consistent with September 26th, 2003 OMB guidance (M-03-22) implementing the privacy provisions of the E-Government Act, agencies must conduct, and submit to OMB, privacy impact assessments for all new or significantly altered information technology investments administering information in identifiable form collected from or about members of the public." Excludes DoD personnel.</p> <p>Applicable" only if a PIA is not required. If "No" is indicated, provide explanation.</p>	Yes, No, NA	Mandatory for all entries for which a PIA is required	PIA
New	PIA_DATE_SUBMIT	8	PIA Date Submitted to OMB. Provide the date the original or updated PIA was submitted to OMB.	YYYYMMDD	Mandatory for all entries for which a PIA is required	PIA
New	PIA_COMMENTS	1000	Free text. Provide explanation for "No" answers to PIA_RVW, PIA_PUBLIC_AVAIL, or PIA_SUBMIT_OMB	Text	Mandatory for any PIA answer is No	PIA
E-Authentication: Changed field names and descriptions, 4 new data elements						

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
New	EAUTH_PUBLIC_ACCESS	1 Logical	Publicly_Accessible. Definition to be promulgated in a future E-Authentication Guidance Memorandum. Yes [there are no technical restrictions for access to the system] No [there are access restrictions such as the use of firewalls, VPN authorization, explicit IP ranges, .mil/.gov domain name restrictions] IF “Yes” is selected, move on to the Authentication Required field. IF “No” is selected, provide an explanation as to why the entry is <u>not</u> Publicly Accessible in the Not Publicly Accessible Explanation field. The system does not meet OMB criteria and should not be reported to OMB.	Yes, No	Mandatory for all	EAUTH
New	EAUTH_NOTPUBLIC_EXPLAIN		Not Publicly Accessible Explanation. Provide an explanation as to why this entry is NOT Publicly Accessible. Specifically, the access restriction to this system/application is: Firewalls VPN Authorization Explicit IP ranges .mil/.gov domain name restrictions Other	Firewalls VPN Authorization Explicit IP ranges .mil/.gov domain name restrictions Other	Mandatory if “No” reported in the Publicly Accessible field	EAUTH
New Field Name	EAUTH_AUTH_RQD	9 Text	Authentication Required. None [no authentication is required to access any part of the system] Partially [authentication is required to access some parts of the system—partially indicates that at least one part of the system requires authentication for access]	None Partially All		EAUTH

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>All [to access all parts of the system requires authentication]</p> <p>IF “All” or “Partially” are selected, move on to E-Authentication Risk Assessment Completed?</p> <p>IF “None” is selected, the system does not meet OMB criteria and should not be reported to OMB.</p>			
New	EAUTH_RISK_ASSESSMENT	Logical	<p>Yes [an E-Authentication Risk Assessment (E-RA) has been performed for the system according to OMB M-04-04, “E-Authentication Guidance for Federal Agencies”]</p> <p>No [an E-RA has not been performed according to OMB M-04-04]</p> <p>IF “Yes” is selected, move on to E-Authentication Risk Assessment Completed/Planned Date.</p> <p>IF “No” is selected, move on to Authentication Method.</p>	Yes, No	Mandatory if “Partially” or “All” reported in the Authentication Required field.	EAUTH
New	EAUTH_RISK_ASSESS_DATE	8 Date	<p>E-Authentication Risk Assessment Completed/Planned Date: The date on which the E-RA was completed for the system, or the date by which the agency plans to have the E-RA completed.</p> <p>After entering the date, move on to the Authentication Method field.</p>	YYYYMMDD	Mandatory if “Yes” is reported in the E-Authentication Risk Assessment Completed field.	EAUTH
New Field Name	EAUTH_AUTHENTICATION_METHOD	15 Text	<p>Identify the lowest level/minimum requirement for authenticating user identity.</p> <p><i>Note: Response will be converted to Assurance Level = 4, 3, 2, 1, 0. This field will determine the assurance level.</i></p>	H/W Crypto Token One-time PW Device Soft Crypto Token Password PIN NA	Mandatory if “Partial” or “All” is reported in EAUTH_AUTH_RQD	EAUTH

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<i>Note: Using a password or PIN to unlock PKI certificate/keys for system authentication is PKI authentication.</i>			
New Field Name Changes from User Entry to automatically generated	EAUTH_ASSURANCE_LEVEL	1 Numeric	The input for this field is <i>automatically</i> derived from the Authentication Method field. H/W Crypto Token = 4 One-Time PW device = 3 Soft Crypto Token = 3 Password = 2 Pin = 1 N/A = 0 Automatically derived from those with an entry in the Authentication Method field. Relationship detailed in Authentication Method field description.	4 3 2 1 0		EAUTH
New Field Name	PK-ENABLED	1 Numeric	PK-Enabled/Planned to be PK Enabled: This field determines when the system is or plans to be PK-enabled for. 1 = No, system is not currently PK-enabled and has no plan to PK-enable. 2 = Yes, system is or will be PK-enabled for user authentication, digital signature, and encryption. 3 = Yes, system is or will be PK-enabled for user authentication and digital signature. 4 = Yes, system is or will be PK-enabled for user authentication and encryption. 5 = Yes, system is or will be PK-enabled for digital signature and encryption. 6 = Yes, system is or will be PK-enabled for user authentication. 7 = Yes, system is or will be PK-enabled for digital signature.	1 2 3 4 5 6 7 8	Mandatory for all	EAUTH

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			8 = Yes, system is or will be PK-enabled for encryption.			
New Field Name	PK_ENABLED_DATE	8 Date	PK-Enabled Date/Expected Date. The date provided in this field would establish when the system was or will be PK-enabled.	YYYYMMDD	Mandatory for all except those with “1” in PK Enabled.	EAUTH
FISMA: 2 new data elements, and changed values for ACCREDITATION_VEHICLE and ACCRED_NOTREQ_EXPLANATION						
New	DATE_ANNUAL SECURITY REVIEW	8 Date	<p>What was the date of the annual security review required by FISMA and DoD?</p> <p>Program officials are responsible for reviewing the security of all systems under their respective control. Clearly, the necessary depth and breadth of an annual system review depends on several factors such as:</p> <ol style="list-style-type: none"> 1) the potential risk and magnitude of harm to the system or data; 2) the relative comprehensiveness of last year’s review; and 3) the adequacy and successful implementation of the POA&M for weaknesses in the system. <p>For example, if last year a system underwent a complete C&A, this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented within the agency. At a minimum, agency officials and CIOs must take into account the three criteria listed above in determining the appropriate level of annual review.”</p>	YYYYMMDD	Mandatory for all entries that are DoD information systems	FISMA
New	SYSTEM_OPERATION	7	Government (DoD) Owned Government Operated (GOGO) Government (DoD) Owned Contractor Operated (GOCO)	GOGO	Mandatory for all entries that are	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>Contractor Owned Contractor Operated (COCO) – includes out-sourced IT services</p> <p>Contractor Owned Government (DoD) Operated (COGO)</p> <p>Non- DoD – includes Federal, State and local governments, grantees, industry partners, etc.</p> <p>FISMA applies to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc. In order to break out agency systems from contractor systems this data field is required.</p>	<p>GOCO</p> <p>COCO</p> <p>COGO</p> <p>NON_DOD</p>	DoD information systems	
Modified	ACCRED_NOTREQ_EXPLANATION	50	<p>Provide an explanation as to why this entry does not require a Certification and Accreditation during its lifecycle.</p> <p>Embedded IT - IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)</p> <p>Integral to real-time execution – IT which is integral to real-time execution of the platform mission (e.g., radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)</p> <p>Without Platform Interconnection - IT which does not communicate outside the platform</p> <p>Pre-deployment – IT that requires Certification and Accreditation but that is still in one of the developmental stages (Concept</p>	<p>Embedded IT</p> <p>Integral to real-time execution</p> <p>Without Platform Interconnection</p> <p>Pre-Deployment</p> <p>Not an IA Record Type</p>	Mandatory for all entries that answer NO to ACCRED_REQUIRED field/FISMA	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>Refinement, Technology Development, System Development & Demonstration) of its life cycle.</p> <p>Not an IA Record type – The entry is not a DoD information system. DODD 8500.1: “For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.”</p>			
Modified	ACCRED_VEHICLE	10	<p>Accreditation Vehicle: Definition – What certification and accreditation (C&A) process was used to grant the current certification and accreditation (C&A)?</p> <ul style="list-style-type: none"> • DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP). The DITSCAP certification and accreditation methodology replaces both AFSSI 5024 (Air Force) and AR 380-19 (Army). • DoD Information Assurance Certification and Accreditation Process (DIACAP) – The future replacement for the DITSCAP • Director of Central Intelligence (DCID) 6/3 • NIST SP 800-37, “Guide for the Certification and Accreditation of Federal Information Systems”, April 2004 • National Industrial Security Program Operating Manual (NISPOM) 	<p>DITSCAP</p> <p>DIACAP</p> <p>DCID 6/3</p> <p>NIST SP 800-37</p> <p>NISPOM</p>	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA

Appendix C –IT Registry Data Elements for Merger

The following data elements currently exist in the DoD IT Registry and will be added into DITPR:

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
No Change	SYSTEM_DESCRIPTOR	1000	A free form text description of the system, its function, and uses.	Free form text	Mandatory for all entries	Core System Info
No Change	DODREGID	8	The DODREGID is an 8-character identifier used to uniquely identify systems in the DoD IT Registry. This unique identifier is created by the Components when a system entry is created. The valid characters in the DODREGID are the uppercase letters and the digits 0 thru 9 [ABCDEFGHJKLMNOPQRSTUVWXYZ0123456789]. The first 2 positions of the 8-character ID are assigned by OSD to each Component in accordance with Table 2. The remaining 6-characters are assigned by the Component. The DODREGID must always contain 8 valid characters.	See Table 2 for allowable values	Mandatory for all entries	Core System Info
No Change	MISSION_CRITICAL	2	<p>The mission criticality of this IT system.</p> <p>Mission Critical - A system that meets the definitions of “information system” and “national security system” in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the USD(C).) A “Mission-Critical Information Technology System” has the same meaning as a “Mission-Critical Information System.” DoDI, 5000.2, May12, 2003.</p> <p>Mission Essential - A system that meets the definition of “information system” in the Clinger-Cohen Act, that the acquiring</p>	MC, ME, MS	Mandatory for all entries	MC/ME

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C).) A “Mission-Essential Information Technology System” has the same meaning as a “Mission-Essential Information System.” DoDI, 5000.2, May12, 2003.</p> <p>Mission Support - Neither Mission Critical nor Mission Essential</p>			
No Change	MAC_CATEGORY	7	<p>Mission Assurance Category (DoDD 8500.1) Definition (from DoDD 8500.1): Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter’s combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:</p> <p>Mission Assurance Category I (MAC I) - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.</p> <p>Mission Assurance Category II (MAC II) - Systems handling information that is important to the support of deployed and</p>	<p>MAC I</p> <p>MAC II</p> <p>MAC III</p>	Mandatory for all entries that are DoD information systems	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			<p>contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.</p> <p>Mission Assurance Category III (MAC III) - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.</p>			
No Change	INTERFACES_IDENTIFIED	3	Indicates if the system interfaces between this entry and other systems have all been identified.	Yes, No, NA	Mandatory for all entries that are DoD information systems	MC/ME
No Change	CONTINGENCY_PLAN	3	Indicates if a contingency plan is in place to account for disruptions in the operations of this system.	Yes, No, NA	Mandatory for all entries that are DoD information systems	MC/ME
No Change	ACCRED_REQ	3	Does this entry require completion of a Department of Defense approved Information Technology Security Certification and Accreditation Process? If any questions, See DoDD 8500.1 Section 2.	Yes, No	Mandatory for all entries that are DoD information systems	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process										
			<p>Examples as they apply to Platform IT or Interconnection Components:</p> <table border="1" data-bbox="686 480 1446 1062"> <thead> <tr> <th data-bbox="686 480 1316 570">Platform IT or Interconnection Components</th> <th data-bbox="1316 480 1446 570">DoDD 8500.1 Applies</th> </tr> </thead> <tbody> <tr> <td data-bbox="686 570 1316 686">IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)</td> <td data-bbox="1316 570 1446 686">No</td> </tr> <tr> <td data-bbox="686 686 1316 859">IT which is integral to real-time execution of the platform mission (e.g., sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)</td> <td data-bbox="1316 686 1446 859">No</td> </tr> <tr> <td data-bbox="686 859 1316 976">IT that is part of or connected with the platform that also connects to external applications that process data in support of the platform (e.g., logistics, training, scheduling, remote diagnostics, etc.)</td> <td data-bbox="1316 859 1446 976">Yes</td> </tr> <tr> <td data-bbox="686 976 1316 1062">IT that is part of or connected with the platform that is part of a defined Information Exchange Requirement (IER) or interfaces with the GIG</td> <td data-bbox="1316 976 1446 1062">Yes</td> </tr> </tbody> </table> <p>If “No” is selected, a reason in the NOTAPPLY_EXPLANATION field is required. Additionally, the following fields do not need to be populated: ACCRED_STATUS, ACCRED_DATE, ACCRED_EXPIRATION, ACCRED_VEHICLE, ACCRED-DOC, SSAA_STATUS, ACCESS_CONTROL, ADMIN_CONTROL, LIFE_CYCLE_PLAN, LIFE_CYCLE_COSTS, MAINTENANCE_PLAN, RISK_PLAN, SECURITY_PLAN,</p>	Platform IT or Interconnection Components	DoDD 8500.1 Applies	IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)	No	IT which is integral to real-time execution of the platform mission (e.g., sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)	No	IT that is part of or connected with the platform that also connects to external applications that process data in support of the platform (e.g., logistics, training, scheduling, remote diagnostics, etc.)	Yes	IT that is part of or connected with the platform that is part of a defined Information Exchange Requirement (IER) or interfaces with the GIG	Yes			
Platform IT or Interconnection Components	DoDD 8500.1 Applies															
IT that is physically part of, internal to, or embedded in a platform used to operate/guide/steer, etc. the platform itself (e.g., avionics, guidance, navigation, flight controls, maneuver control, navigation, etc.)	No															
IT which is integral to real-time execution of the platform mission (e.g., sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition (SCADA) systems)	No															
IT that is part of or connected with the platform that also connects to external applications that process data in support of the platform (e.g., logistics, training, scheduling, remote diagnostics, etc.)	Yes															
IT that is part of or connected with the platform that is part of a defined Information Exchange Requirement (IER) or interfaces with the GIG	Yes															

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			CSIRT, SECURITY_CONTROL_TEST, VIRUS_PROTECTION, DAA_NAME, DAA_TITLE, DAA_ORG, DAA_PHONE, DAA_EMAIL.			
No Change	ACCRED_STATUS	10	<p>Accreditation Status: Definition – Has your system undergone a certification and accreditation process and if so, what is its current status?</p> <ul style="list-style-type: none"> • ATO – Authority to Operate • IATO – Interim Authority to Operate • IATT – Interim Authority to Test • DATO – Denial of Authority to Operate • None – Not Yet Accredited 	ATO IATO IATT DATO None	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ACCRED_DATE	8	<p>Accreditation Date: Definition – On what date was the current certification and accreditation (C&A) status granted?</p> <p>**If system has no accreditation, enter the projected accreditation dates. Future dates automatically cause ACCRED_STATUS field to be set to “None.”</p>	YYYYMMDD	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ACCRED_EXPIRATION	8	<p>Accreditation Expiration Date: Definition – When is the current certification and accreditation (C&A) set to expire?</p> <p>A Final Accreditation expiration date cannot exceed 3 years from the value in the ACCRED_DATE field</p> <p>An IATO Accreditation expiration date cannot exceed 1 year from the value in the ACCRED_DATE field</p>	YYYYMMDD	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ACCRED_DOC	3	<p>Formal Documentation: Definition – If your system has a certification and accreditation (C&A), do you have formal documentation that indicates the specifics of the certification and accreditation (C&A) process?</p>	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
No Change	SSAA_STATUS	4	<p>Systems Security Authorization Agreement (SSAA) Status: Definition – What phase is the SSAA associated with your system in? The phases of the SSAA are based on Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) definitions.</p> <p>Phase I - The Definition Phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority (DAA) and Certification Authority (Certifier), and document the C&A security requirements. Phase I culminates with a documented agreement between the Program Manager, DAA, Certifier, and user representative on the approach and results of the Phase I activities.</p> <p>Phase II - The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (h)), there is a corresponding set of security activities that verifies compliance with the security requirements and constraints and evaluates vulnerabilities.</p> <p>Phase III - The Validation Phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. Validation culminates in an approval to operate.</p> <p>Phase IV - The Post Accreditation Phase includes activities to monitor system management, configuration, and changes to the operational and threat environment to ensure an acceptable level of residual risk is preserved. Security management, configuration</p>	I II III IV	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			management, and periodic compliance validation reviews are conducted. Changes to the system environment or operations may warrant beginning a new DITSCAP cycle.			
No Change	CONTINGENCY_TEST	8	Contingency Plan/Continuity of Operations Plan (COOP) last exercised: Definition – When was the last time that your system’s contingency plan/COOP was exercised?	YYYYMMDD	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ACCESS_CONTROL	3	Access Controls: Definition – Does your system have measures in place that control access and prevent the circumvention of the security software and application controls?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ADMIN_CONTROL	3	Administrative Controls: Definition – Does your system have measures in place that ensure the proper administration of your system to include identification of users, groups, and their privileges as well as the capability to produce system activity audit logs?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	LIFE_CYCLE_PLAN	3	System Life Cycle Plan: Definition – Does your system have a life cycle plan that discusses at minimum the basic life cycle phases?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	LIFE_CYCLE_COSTS	3	Life Cycle Costs – Indicate whether your system has the costs of its security controls into the life cycle of the system.	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	MAINTENANCE_PLAN	3	Hardware/Software Maintenance Plan: Definition – Does your system have controls that are used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	RISK_PLAN	3	Risk Management Plan: Definition – Does your system have a risk management plan that identifies the risks and vulnerabilities to the system, recognizes the sensitivity of the data and lays out a plan to	Yes, No, NA	Mandatory for all entries that answer “Yes” to	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			mitigate those risks and vulnerabilities?		ACCRED-RQD	
No Change	SECURITY_PLAN	3	System Security Plan: Systems Security Authorization Agreement (SSAA) in accordance with DITSCAP (DoDI 5200.40 and DoD 8510.1-M). Definition – Does your system have a system security plan that provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements? Does the plan delineate responsibilities and expected behavior of all individuals who access the system?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	CSIRT	3	Computer Security Incident Response Team (CSIRT): Definition – Does your system have controls (e.g. Security Incident Response Team, etc.) in place to recognize, report, monitor and efficiently handle incidents, and is there a capability to share this information with appropriate organizations?	Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	SECURITY_CONTROL_TEST	8	<p>Security Controls Tested – Indicate the last date system security controls were tested.</p> <p>SSAA should document the initial and subsequent testing and validation. FISMA requires evaluation annually. DoDI 8500.2 controls provide additional basis for evaluation.</p> <p>Management Controls - Controls that address the security management aspects of the IT system and the management of risk for the system</p> <p>Operational Controls - Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems)</p> <p>Technical Controls - Controls that address security mechanisms contained in and executed by the computer system</p>	YYYYMMDD	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
No Change	VIRUS_PROTECTION	3	Virus Protection: Definition – Does your system have virus protection and data integrity controls that protect data from accidental or malicious alteration or destruction and that protect your system from infection from malicious computer viruses?	FISMA Yes, No, NA	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	ENTRY_DATE	8	Date a record was created in the IT Registry to store information about this system. For future entries, the date will be automatically assigned upon entry into the Registry.	YYYYMMDD	Applies to new entries only	FISMA
No Change	POA&M_REQUIRED	1 Logical	Does this entry require a security POA&M due to unresolved security weaknesses? Refer to FY05 FISMA guidance for POA&M guidance. In general, operational systems without an ATO require a POA&M. Definition - Plan of Action and Milestones (POA&M) A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in IT programs and systems.	Yes, No	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	DATE_SUBMITTED	8	Provide the date the original or updated POA&M was provided to the Component CIO. POA&Ms are to be updated quarterly until all security weaknesses are closed.	YYYYMMDD	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA
No Change	CONFIDENTIALITY_LEVEL	10	From DODI 8500.2, February 6, 2003. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may	Classified Sensitive Public	Mandatory for all entries that answer “Yes” to ACCRED-RQD	FISMA

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO	Supported IT Process
			access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: classified, sensitive, and public.			

The following data elements currently exist in the DoD IT Registry, will not be added into DITPR, and will be removed from the SIPRNET DoD IT Registry:

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO
Deleted	USI	10	Universal System Identifier (USI) – A unique system identifier that is assigned to each unique system in the DoD IT Registry and the DoD Systems Index database. This is the crosswalk field between the IT Registry and the DoD Systems Index database. Eventually, the USI will be used to index all DoD information systems across all DoD databases. This field is still in the development phase. NOTE: Do not use this field until guidance is promulgated by OASD(NII).		Assigned by DoD IT Registry (currently in development)
Deleted	SYSTEM_ID	20	The distinct System Identification Number or Code used on the Component's database for this entry.		Optional for all entries
Deleted	FUNC_AREA	50	Relates to the functions under which this particular entry is reported.	See Table 4	Mandatory for all entries
Deleted	SEC_FUNC_AREA	50	For use if this entry has a secondary function.	See Table 4	Mandatory for all entries
Deleted	TERC_FUNC_AREA	50	For use if this entry has a tertiary function.	See Table 4	Mandatory for all entries
Deleted	GIG_COMPLIANT	3	NO = needs a waiver. YES = no waiver required NA = waiver not applicable due to type of system (i.e., weapons) NOTE: Do Not enter data into this field unless directed by Office of the	Yes, No, NA	Optional, only at the request of OSD

Appendix C –IT Registry Data Elements for Merger

STATUS	FIELD NAME	FIELD SIZE	FIELD DESCRIPTION	FIELD FORMAT	APPLIES TO
			Assistant Secretary of Defense (NII)		
Deleted	WAIVER_EXPIRATION_DATE	8	Means a waiver has been issued and will expire on this date. This will be a flagged field to remind the component and the waiver panel of this date. NOTE: Do Not enter data into this field unless directed by Office of the Assistant Secretary of Defense (NII)	YYYYMMDD	Optional, only at the request of OSD
Deleted	WAIVER_REVIEW_DATE	8	Waiver must be reviewed on this date. Means the component must come before that month's GIG Waiver Panel to renew its waiver or it will expire. This will be a flagged field to remind the waiver panel and the component of this date. NOTE: Do Not enter data into this field unless directed by Office of the Assistant Secretary of Defense (NII)	YYYYMMDD	Optional, only at the request of OSD

Appendix C –IT Registry Data Elements for Merger

Table 1: Acceptable Values for Components/Others

Services	Defense Agencies	Field Activities	Other
Army	DARPA	AFIS	ASD(HA)
Navy	DFAS	CIFA	ASD(LA)
USMC	DIA	DHRA	ASD(RA)
USAF	DISA	DoDEA	ASD(PA)
	DeCA	DPMO	ASD(HD)
	DCAA	DTIC	ASD(ISA)
Combatant Commands	DLA	DTRMC	ASD(NII)
CENTCOM	DCMA	DTSA	ASD(ISP)
EUCOM	DLSA	OEA	ASD(SO/LIC)
JFCOM	DSCA	TMA	GC
NORTHCOM	DSS	WHS	DOT&E
PACOM	DTRA		DODIG
SOCOM	MDA	Other	USNATO
SOUTHCOM	NGA	OSD(CIO)	NCBDP
STRATCOM	NSA	NRO	EXECSEC
TRANSCOM	PFFA	USD(AT&L)	INTEL OVERSIGHT
		USD(P)	DA&M
Joint Staff		USD(C)	DPA&E
		USD(P&R)	DNA
		USD(I)	DFT
			NGB

Appendix C –IT Registry Data Elements for Merger

Table 2. Instructions for DODREGID

DoD COMPONENT		ID Range
ACRONYM	TITLE	
AFIS	Armed Forces Information Service	AA
Army	United States Army	AB
MDA	Missile Defense Agency	AC
CENTCOM	United States Central Command	AD
CIFA	Defense Counterintelligence Field Activity	BX
DARPA	Defense Advanced Research Projects Agency	AE
DCAA	Defense Contract Audit Agency	AF
DCMA	Defense Contract Management Agency	AG
DeCA	Defense Commissary Agency	AH
DFAS	Defense Finance and Accounting Service	AI
DHRA	Defense Human Resources Activity	AJ
DIA	Defense Intelligence Agency	AK
DISA	Defense Information Systems Agency	AL
DLA	Defense Logistics Agency	AM
DSCA	Defense Security Cooperation Agency	AO
DSS	Defense Security Service	AP
DTIC	Defense Technical Information Center	BU
DTRA	Defense Threat Reduction Agency	AQ
DTRMC	Defense Test Resource Management Center	BV
DTSA	Defense Technology Security Administration	BW
EUCOM	United States European Command	AS
JFCOM	United States Joint Forces Command	AT
Joint Staff	Joint Staff	AU
Navy	United States Navy	AV
NGA	National Geospatial-Intelligence Agency	AW
NORAD	North American Aerospace Defense Command (under NORTHCOM)	AX
NRO	National Reconnaissance Office	AY
NSA	National Security Agency	AZ
OSD (ALL)	Office of the Secretary of Defense (All OSD Staff Components)	BB
PACOM	United States Pacific Command	BC
SOCOM	United States Special Operations Command	BD
SOUTHCOM	United States Southern Command	BE
STRATCOM	United States Strategic Command	BG
TRANSCOM	United States Transportation Command	BH
USAF	United States Air Force	BI
USFK	United States Forces Korea (under PACOM)	BJ
USMC	United States Marine Corps	BK
WHCA	White House Communications Agency (under DISA)	BL
WHS	Washington Headquarters Service	BM

Appendix C –IT Registry Data Elements for Merger

DoD COMPONENT		ID
ACRONYM	TITLE	Range
NORTHCOM	United States Northern Command	BN
DoDEA	Department of Defense Education Activity	BO
DLSA	Defense Legal Services Agency	BP
PFFA	Pentagon Force Protection Agency	BQ
DPMO	Defense POW/Missing Personnel Office	BR
OEA	Office of Economic Adjustment	BS
TMA	Tri-Care Management Activity	BT
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics	DA
USD(P)	Under Secretary of Defense for Policy	DB
USD(C)	Under Secretary of Defense (Comptroller)/Chief Financial Officer	DC
USD(P&R)	Under Secretary of Defense for Personnel and Readiness	DD
USD(I)	Under Secretary of Defense for Intelligence	DE
ASD(HA)	Assistant Secretary of Defense (Health Affairs)	BA
ASD(HD)	Assistant Secretary of Defense (Homeland Defense)	DF
ASD(ISA)	Assistant Secretary of Defense (International Security Affairs)	DG
ASD(ISP)	Assistant Secretary of Defense (International Security Policy)	DH
ASD(LA)	Assistant Secretary of Defense (Legislative Affairs)	DI
ASD(PA)	Assistant Secretary of Defense (Public Affairs)	DJ
ASD(RA)	Assistant Secretary of Defense (Reserve Affairs)	DK
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)/DoD CIO	DL
ASD(SO/LIC)	Assistant Secretary of Defense (Special Operations/Low Intensity Conflict)	DM
DOT&E	Director, Operational Test and Evaluation	DN
DA&M	Director, Administration and Management	DO
DPA&E	Director, Program Analysis and Evaluation	DP
DNA	Director, Net Assessment	BY
DFT	Director, Force Transformation	BZ
GC	General Counsel of the Department of Defense	DQ
DoDIG	Inspector General of the Department of Defense	AN
USNATO	U.S. Mission to NATO	DT
NCBDP	Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs	DR
EXECSEC	Executive Secretary of the Department of Defense	DS
NGB	National Guard Bureau	DZ

Appendix D – DITPR Data Elements to be Completed for Systems Added from the DoD IT Registry

Data elements in DITPR to be completed for systems added from the DoD IT Registry that did not already have a DITPR entry will be conducted as follows:

For non-Defense Business Systems:

- DITPR Data Elements to be populated by March 1, 2006:
 - Type of IT Investment (e.g., Business System, Infrastructure, NSS, Initiative, not applicable)
 - IRB/Mission Area (Warfighting, Intelligence, Enterprise Information Environment (EIE), or Business Mission Area).
 - Type of National Security System

- DITPR Data Elements to be populated by June 1, 2006 (if pick lists are available):
 - IRB/Mission Area Role (Domain or Core Business Mission Area)
 - Operational Activities
 - Function Type

For Defense Business Systems:

- All Defense Business Systems must be entered into DITPR by December 31, 2005.
- For Tier 4 Defense Business Systems the DITPR Data Elements that must be populated are:
 - Component
 - System Name
 - System Acronym
 - System Description
 - IRB Mission Area
 - IRB/Mission Area Role (Primary and any Partners/Secondary)
 - Budget Initiative Number (BIN) (from SNaP-IT)
 - Transition Plan State (Core, Interim or Legacy system)
 - IRB Tier
 - Type of IT Investment (e.g., Business System, Infrastructure, NSS, Initiative, not applicable)
 - Type of National Security System
 - System Lifecycle Phase (LIFE_CYCLE in DoD IT Registry)
 - ACAT Category
 - Operational Activities
 - Function_Type
 - IT Registry Number (DODREGID in DoD IT Registry) (if applicable)
 - Mission Critical (MC/ME data element from DoD IT Registry)
 - Contingency Plan (MC/ME data element from DoD IT Registry)
 - Interfaces Identified (MC/ME data element from DoD IT Registry)

Appendix D – DITPR Data Elements to be Completed for Systems Added from the DoD IT Registry

- POC Information

- Defense Business Systems not in the DoD IT Registry by December 16, 2005 must complete FISMA, PIA, and E-Authentication data elements by March 1, 2006.

Appendix E – Detailed Instructions and Milestones

1. Detailed Instructions:

a. Merge of systems from DoD IT Registry into DITPR:

- (1) Criteria to determine if a record exists in both the DoD IT Registry and DITPR:
 - Same Component and Acronym
 - DODREGID number in DITPR matches DODREGID in DoD IT Registry
 - If all 3 do not match, consider DITPR to not be populated and add the record from the ITR.
 - If all 3 match, check other “common data”
- (2) Criteria for considering “common data” to be a match:
 - Same System Name, BIN (if populated), ACAT, Life Cycle
 - If all 4 match, add DoD IT Registry data to the DITPR record
 - If all 4 do not match, move to Component Holding Area
- (3) Component Holding Area Business Rules:
 - Components have 30 days to determine which data elements should be used to populate DITPR
 - At end of 30 day period, data in DoD IT Registry record will be used to overwrite the DITPR data for the common data elements that do not match.
- (4) Components will have until March 1, 2006 to resolve any duplicate system entries.

b. DoD IT Registry Operations.

- (1) NIPRNET: On December 16, 2005, the DoD IT Registry will be locked as follows:
 - Edit and upload access will be terminated
 - Download and read only access will be permitted until January 31, 2006 when the NIPRNET version of the DoD IT Registry will cease operation.
 - No new user accounts will be issued.
- (2) SIPRNET: The SIPRNET version of the Registry will continue operations as currently configured; however, batch upload capability will be disabled. The data dictionary in Appendix C will be implemented on January 31, 2006.

Appendix E – Detailed Instructions and Milestones

2. Milestones.

Action/Event	Who	Date	Comments
Combine DoD IT Registry Tiger Team with Technical Solutions IPT	NII/Components	September 28, 2005	Begin bi-weekly combined meetings
Identify Merger POC	Components	October 1, 2005	All Components will need to designate a Sponsor and Admin
Merger Meeting	NII/Components	October 12, 2005	Review merger guidance memo in detail
Technical Solutions IPT Meeting	NII/Components	October 26, 2005	Review status of merger
Complete testing with Components	DITPR Team	October 28, 2005	
Request DITPR Accounts	Components	October 31, 2005	Component Admin in DITPR will apply permissions based on user roles
Component users attend training	Components/ DITPR Team	October 24-28, 2005	Dates and Locations TBD
First Load of IT Registry systems into DITPR	ITR/DITPR Teams	October 31, 2005	
Resolve data for systems in holding area	Components	November 1 – December 1, 2005	
Technical Solutions IPT Meeting	NII/Components	November 23, 2005	Review status of merger; status of adding 50% MS systems
Quarterly Update of IT Registry	Components	NLT December 1, 2005	Includes at least 50% of Mission Support systems
COI Kickoff Meeting	NII/Components	(T) December 7, 2005	
Quarterly FISMA Report to OMB	NII/DCIO/DIAP	December 15, 2005	

Appendix E – Detailed Instructions and Milestones

Action/Event	Who	Date	Comments
All Tier 4 Defense Business Systems added to DITPR	Components	December 16, 2005	Data elements to be populated per Appendix D
Second Load of IT Registry systems into DITPR	ITR/DITPR Teams	December 16, 2005	Lock IT Registry when load completed. Read Only access and Download allowed; no edits, uploads, or new accounts.
Technical Solutions IPT Meeting	NII/Components	January 4, 2006	Review status of merger, DITPR
Resolve data for systems in holding area	Components	December 17, 2005 – January 15, 2006	
Technical Solutions IPT Meeting	NII/Components	January 18, 2006	Review status of merger
DITPR becomes official unclassified DoD data source	DoD	January 31, 2006	FISMA, PIA, E-Authentication, Portfolio Management, MC/ME, DODI 5000.2 system registration
Data element additions and changes applied to SIPRNET IT Registry	ITR Team	January 31, 2006	
Archive DoD IT Registry (NIPRNET); cease operations	ITR Team	February 1, 2006	SIPRNET will continue to operate in online mode. Download will be available but no batch uploads.
Technical Solutions IPT Meeting	NII/Components	February 1, 2006	Review status of DITPR
Duplicate entries in DIPTR resolved	Components	March 1, 2006	

Appendix E – Detailed Instructions and Milestones

Action/Event	Who	Date	Comments
Phase I of DITPR data fields populated for non-Defense Business Systems added from IT Registry	Components	March 1, 2006	<ul style="list-style-type: none"> • Type of IT Investment • IRB/Mission Area • Type of National Security System
Phase II of DITPR data fields populated for non-Defense Business Systems added from IT Registry	Components	June 1, 2006 (if pick lists are available)	<ul style="list-style-type: none"> • IRB/Mission Area Role • Operational Activities • Function Type