DoD CIO Interoperability Process

30 Apr 2012

Ed Zick
DoD CIO
edward.zick@osd.mil
(571) 372-4680
4. TITLE AND SUBTITLE  
**DoD CIO Interoperability Process**

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)  
Department of Defense Chief Information Officer (DoD CIO), Washington, DC, 20301

12. DISTRIBUTION/AVAILABILITY STATEMENT  
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES  
Presented at the 2012 DoD Enterprise Architecture, Miami, FL, April 30 - May 3, 2012

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:
   a. REPORT  
   unclassified
   b. ABSTRACT  
   unclassified
   c. THIS PAGE  
   unclassified

17. LIMITATION OF ABSTRACT  
Same as Report (SAR)

18. NUMBER OF PAGES  
15

Standard Form 298 (Rev. 8-98)  
Prescribed by ANSI Std Z39-18
Purpose

The purpose of this brief is to:

• Describe the Enhanced Information Support Plan (EISP) Enterprise Service Version (ESV), a module within the GIG Technical Guidance Federation (GTG-F)

• Describe the benefits users experience when using the GTG-F to create and submit ISPs for review and approval

• Explain how the DoD CIO utilizes the EISP to collect and analyze information to assess interoperability compliance
The DoD CIO has released Interim Guidance for Interoperability and prescribed use of the GTG-F

Interim Guidance for the Interoperability of Information Technology (IT) and National Security Systems (NSS) was signed 27 March 2012


Unclassified ISPs shall be created, submitted, and approved using the GIG Technical Guidance Federation (GTG-F)

The GTG-F is available for use: https://gtg.csd.disa.mil

- Common Access Card (CAC) authentication is required to access the GTG-F

GTG Federation Processes for ISP Development and Assessment of IT and NSS:

- Wednesday, Track 1, 1615 – 1700
- Demonstration of the GTG-F, including an overview of the EISP, GTP, and IAM

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHIEF OF STAFF OF THE ARMED FORCES
AND ASSISTANT SECRETARIES OF DEFENSE
AND COMMANDING OFFICERS, MILITARY DEPARTMENTS

SUBJECT: Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)

Reference: “Memorandum of Understanding Between the Joint Staff, the Director of the Department of Defense Information Systems Agency (DISA), and the Department of Defense Chief Information Officer for Transfer of Functions and Associated Resources,” August 26, 2011

Reference transferred specific functions from the Joint Staff (JS) to the DoD CIO to include responsibilities for interoperability of IT and NSS previously performed by the Joint Staff [6]. The purpose of this memorandum is to provide interim guidance for the review and approval of Information Support Plans (ISPs), and interoperability certification of IT and NSS. This interim guidance memorandum does not alter existing DoD authorities or command relationships.

The DoD CIO point of contact for this action is Mr. Kris Stranze, kris.stranze@osd.mil, 571-372-4678.

Terena M. Takai

Attachment:
Interim Guidance for Interoperability of IT and NSS

UNCLASSIFIED
The DoD CIO, in partnership with DISA, has developed and instituted the GTG-F to create a more efficient and effective Interoperability assessment process.

- The GTG-F is hosted on the DISA DECC, driven by the Enhanced Information Support Plan (EISP), enabling compliance with the DoD Information Enterprise Architecture (DIEA), GTPs, and DoD IT Standards Registry (DISR) IT standards.
- The data captured within the EISP and GTP module is pushed to the Interoperability Assessment Module (IAM) which provides a streamlined staffing, review, and commenting process for Interoperability data.
- The GTG-F incorporates benefits of cloud computing, allowing users:
  - Access to the Federation from “anywhere” while protecting programmatic data via PKI CAC authentication
  - To collaborate with other GTG-F users on a single program
  - The ability to share information via Web Service

There are over 140 active programs in the GTG-F (as of 27 April 2012)
The GTG-F provides PMs with a data-centric interoperability and compliance analysis process

- Guides PMs to better identify interoperability risks, issues, and develop mitigation plans through the use of online templates, business rules, and data validation capabilities
- Automates some architecture imports from tools or repositories reducing duplication of effort and provides visibility into information needs, dependencies, and interface requirements, focusing on interoperability and integration
- Eliminates the need to manually produce a document for submission as the data entered into the process is automatically formatted for review
- Implements an online review process allowing PMs and reviewers real-time adjudication of comments made directly on the data thus reducing administrative and duplicative comments
- Automatic triggers ensure information risks are identified, standards are current, and other mandatory compliance areas are assessed
- Provides the DoD an efficient, data-centric process for collecting and standardizing interoperability information while providing a single repository through which the DoD can perform analysis and increase decision speed

Stryker Brigade Combat Team realized a **30-40% cost savings** in development of their ISP via this data-centric process

Joint Staff ISP reviewers said **EISP generated ISPs are more thoroughly written** and do not lack required detail as often as legacy ISPs

OSD(Health Affairs)/TRICARE Management Activity is **saving time and effort** by reusing data from Version 2.0 by utilizing the XML import capability within the EISP ESV
The EISP enables interoperability and compliance risk assessment within the acquisition process

- The EISP is the DoD CIO’s **primary source** to collect and analyze information to ensure interoperability and compliance in these areas:
  - Integrated Architecture
  - DoD Information Enterprise Architecture
  - Standards
  - Net-Centric Strategy
  - Information Assurance
  - Web Services
  - Secure Information Exchanges

- Interoperability and compliance risk assessment provides the DoD CIO a **methodology to assess compliance** in the DoD Decision Support System

This data is being used as part of the DoD CIO’s Technical Assessment on the IT Dashboard

Also, this data is being used to develop the DoD CIO position regarding program development and delivery for OIPTs, IRBs and DABs
Integrated Architecture

- The EISP Process Analysis section uses a program’s architecture data to perform analysis that drives a PM to identify risks and issues within their program.

- The EISP captures program architecture data across the Enterprise, in a standard format, to allow for the sharing and reuse of ISP information as well as for cross-program and Portfolio-level analysis.

DoD Architecture Framework (DoDAF)
The EISP ESV allows users to import data into the Process Analysis section to reduce the burden on ISP developers and to assist in the DoD CIO’s risk and issue analysis.

- In the Process Analysis section, the ISP developer is asked to enter their detailed warfighter or business process related data:
  - The EISP ESV contains the ability to automatically import pieces of required data directly into the Process Analysis section, reducing the amount of manual data entry.
  - The information collected by the DoD CIO drives PMs to identify risks and issues that, if not properly managed, will limit or restrict the ability of a program to be operationally employed in accordance with requirements.
DoD Information Enterprise Architecture

- The EISP collects the data elements required by the DoD IEA and allows users to tailor the DoD IEA Activity model to their specific program.

- The EISP automatically generates the DoD IEA Compliance Assessment Table from the data entered in the process.

- DoD IEA V2.0 requirements are being researched and generated for a future EISP release.

DoD Information Enterprise Architecture (DoD IEA) Version 1.2
http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx
Standards

- The GTG-F GIG Technical Profiles Wiki is located at: https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG_GTPs
Net-Centric Data Strategy

- The EISP collects information to analyze and assess a program’s compliance with the Net-Centric Data Strategy through the collection of Data Sharing Characteristics:
  - DDMS
  - MDR Registered
  - Web Service
  - NCES Registered
  - Discoverable
  - IPv6 Capable
  - Tagged

DAG Ch. 7.4 Net-Centric Information Sharing Data Strategy
The EISP collects references to a program’s IA Strategy and PPP so that reviewers and analysts may access the IA information they require. By doing so, the EISP does not recreate IA information that exists in an authoritative data source. Through analysis of Minimum Parameters, the EISP is able to analyze IA at the critical link level.

IA Policies for reference:
- DoDD 5000.1 The Defense Acquisition System
- DODI 5000.2 Operation of the Defense
- DODD 8500.01E Information Assurance
- DoDI 8500.2 Information Assurance Implementation
- DoDI 8580.1 Information Assurance in the Defense
- DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process
- DoDI 5200.40 DoD Information Technology Security Certification and Accreditation Process

Information Assurance Policy References
GTG-F Configuration Control Board (CCB) will be stood up to incorporate feedback, changes, and policy updates into the process

- The GTG-F CCB will include members from the DoD CIO, DISA, and the DoD Components
  - Members will provide inputs as to which changes and enhancements should be included in each release

- Users may add new GTG-F requirements in the GTG-F Software Forge community: [https://software.forge.mil/sf/projects/gtg_f](https://software.forge.mil/sf/projects/gtg_f)

- The EISP is continuing to evolve and bring additional capabilities online, including:
  - Additional, and improved, architecture imports to reduce burden on PMs
  - Streamlined PDF to reduce size and complexity of ISP output

- The EISP will be updated to accommodate new policy and guidance
  - CJCSCI 6212.01F
  - DoD IEA Version 2.0
Summary

• The Interim Guidance for the Interoperability of Information Technology (IT) and National Security Systems (NSS), signed 27 March 2012, prescribes the use of the GTG-F to create and submit ISPs and GTPs for review and approval
  – [https://gtg.csd.disa.mil](https://gtg.csd.disa.mil)

• The GTG-F provides PMs with a data-centric interoperability compliance analysis process that saves ISP developers time and money vs. the legacy process through the automatic import of architecture data, use of online templates, business rules, and data validation capabilities, and references to authoritative data sources

• The EISP, and the GTG-F, will continue to evolve to incorporate new capabilities, streamline the process for PMs, and create an effective and efficient process to collect Interoperability data

• POCs
  
  EISP Help Desk  
  eisp_help@bah.com

  GTG-F Help Desk  
  EE3TechSupport@disa.mil