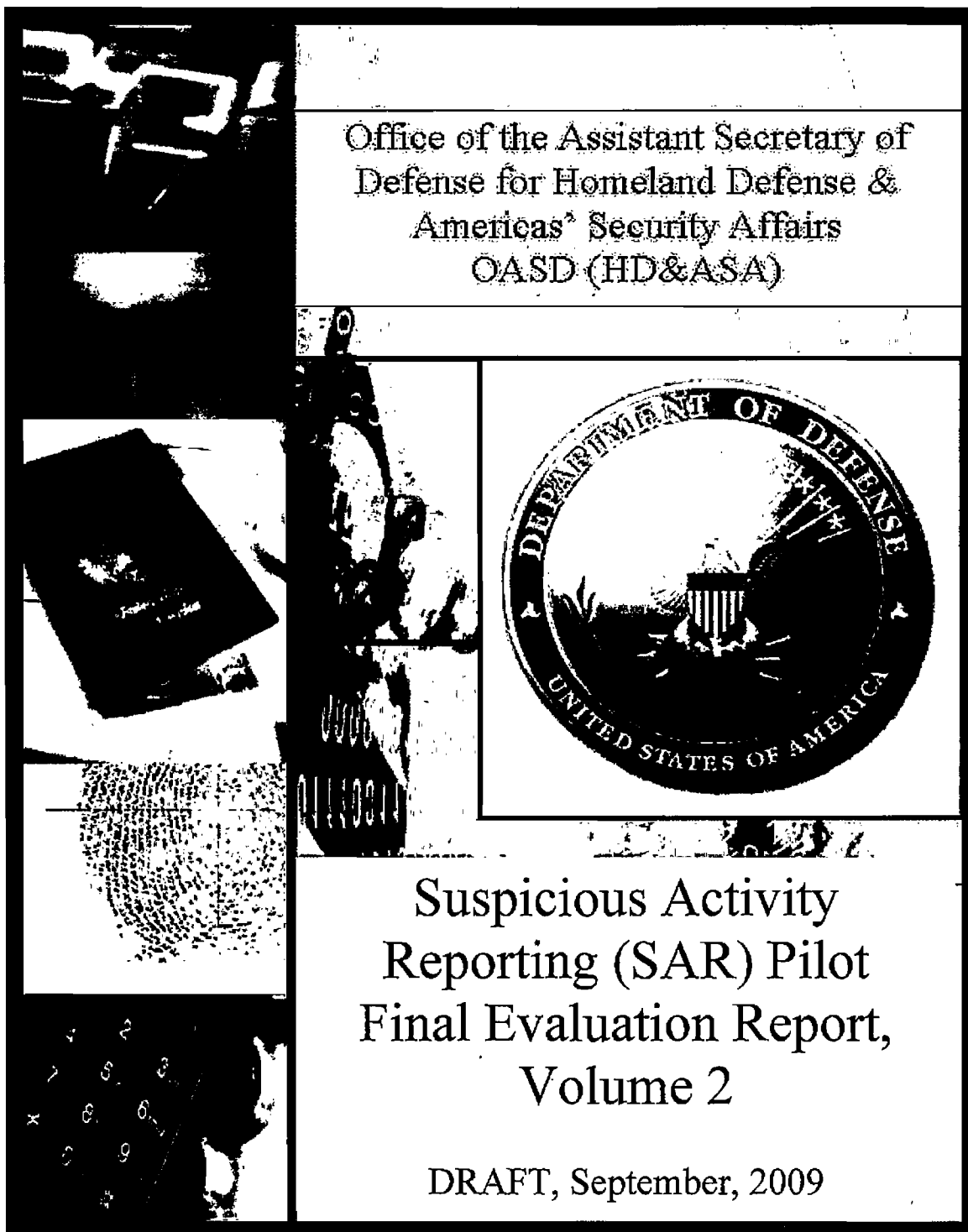




EGuardian-576

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Table of Contents

1	Introduction.....	1
2	List of References	1
2.1	General	1
2.2	DoD and Other Policy References	1
2.3	FBI Technical References	2
3	Acronyms.....	4
Appendix E	eGuardian System and Software Description	6
E.1	General Overview	6
E-2	eGardian Functionality.....	6
E.3	Software Architecture and Design	7
E.4	System Design.....	9
E.5	Network Design.....	10
E.6	Development Environment	10
E.6.1	Testing Procedures	10
E.6.3	Configuration Control	11
E.7	Operational Considerations.....	11
E.7.1	Configuration Control	11
E.7.2	Failover Scheme.....	12
E.7.3	Disaster Recovery	12
E.8	Evaluation Discussion.....	12
Appendix F	eGuardian Net Centric Features Evaluation.....	13
F.1	Summary	13
F.2	Data	16
F.3	Services	25
F.4	Information Assurance	27
Appendix G	eGuardian Privacy Evaluation.....	32
Appendix H	eGuardian Security Evaluation	34

List of Tables

No table of figures entries found.

List of Figures

Figure E-1. eGuardian Logic Diagram	6
---	---

1 Introduction

This Volume 2 of the Office of Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, *Suspicious Activity Reporting (SAR) Pilot Final Evaluation Report* contains the technical evaluation of the eGuardian system. The Appendix E is a description of the system, its development and release methods, and software configuration control. This is followed by the assessments of its compliance with Net Centric guidance (Appendix F), its compliance with the privacy impact assessment (Appendix G), and compliance with DoD security guidance (Appendix H).

2 List of References

The references below were referenced in this document or used as supportive information.

2.1 General

1. DoD Homeland Defense & Americas' Security Affairs; eGuardian Application "Quick Look"; 3/31/2009; Prepared for DoD by the MITRE Corporation.
2. The DoD SAR Evaluation Plan, DRAFT December 2008, Prepared for DoD by the MITRE Corporation.
3. Survey sample tools (calculator, formula, significance, survey design, results correlation) available at "Creative Research Systems"; <http://www.surveysystem.com/signif.htm>, used December 2008 and March 2009).
4. The DoD SAR Interim Evaluation Report, 31 March 2009, Prepared for DoD by the MITRE Corporation.
5. TALON Termination and Transition Group (T3G), Technical Assessment of Suspicious Activity Reporting (SAR) Systems, SUPPLEMENT: COMPLETED EVALUATION CHECKLISTS AND KEY DECISION POINTS, March 2008, Prepared for: Office of the Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs OASD(HD&ASA) by ANSER [Analytic Services, Inc.]
6. TALON Termination and Transition Group (T3G), Technical Assessment of Suspicious Activity Reporting (SAR) Systems, Analysis Process of Suspicious Activity Reporting (SAR) Systems, August 2008, Prepared for: Office of the Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs OASD(HD&ASA) by ANSER
- 7.

2.2 DoD and Other Policy References

1. Deputy Secretary of Defense, Memorandum, Directive-Type Memorandum (DTM) 08-007 – DoD Force Protection Threat Information, July 22, 2008.
2. Deputy Secretary of Defense, Memorandum, Implementation of Interim Threat Reporting Procedures, September 13, 2007.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

3. Department of Defense, Memorandum, Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance, October 28, 2005.
4. Department of Defense, DD Form 2930, PRIVACY IMPACT ASSESSMENT (PIA), November 2008.
5. DoDI 8500.2, Department of Defense, Instruction, Information Assurance (IA) Implementation, February 6, 2003.
6. DoD, DISA, *Database Security Technical Implementation Guide*, Version 8, Release 1, 19 September 2007
7. DoD, DISA, *Web Server Security Technical Implementation Guide*, Version 6, Release 1, 11 December 2006.
8. DoD, DISA, *Enclave Security Technical Implementation Guide*, Version 4, Release 2, 10 March 2008.
9. DoD, DISA, *UNIX Technical Implementation Guide*, Version 5, Release 1, 28 March 2006.
10. DoD, DISA, *Access Control in Support of Information Systems Technical Implementation Guide*, Version 2, Release 2, 26 December 2008.
11. *Developed by DISA for the DoD* Department of Defense, Chief Information Officer, The Pentagon—Washington, D.C., *Net-Centric Services Strategy for a Net-Centric, Service Oriented DoD Enterprise*, May 4, 2007.
12. Department of Defense, Chief Information Officer (CIO), *Net-Centric Data Strategy*, May 9, 2003.
13. Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, *Net-Centric Checklist*, Version 2.1.3, May 12, 2004
14. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*, April 2000.
15. *Information Sharing Environment Guidance (ISE-G), Identity and Access Management Framework for the ISE*, Version 1.0

2.3 FBI Technical References

1. Selected Slides from eGuardian V1.0, BiWeekly Project Status, May 23, 2008, [redacted] and [redacted]
2. Federal Bureau of Investigation (FBI), *eGuardian 1.0, Appendix to FTTTF Techtrack Network System Security Plan*, July 10 2008, Version 2.3.
3. [redacted] Threat Monitoring Unit (TMU), *Privacy Impact Assessment for the eGuardian Threat Tracking System*, Counterterrorism Division, July 11, 2008.
4. FBI Security Division, Information Assurance Section, *FBI Certification and Accreditation Handbook*, Version 3.0, June 29, 2007. (Chapter 2 – Certification and Accreditation Authorities and Roles)
5. FBI Security Division, *Security Policy Manual*.
6. FBI *System Security Plan (SSP) Template*. Version 3.

b6 per FBI
b7c

EGuardian-579
UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Federal Bureau of Investigation (FBI), eGuardian 1.0, Appendix to FTTTF Techtrack Network System Security Plan, Version 2.3, July 10, 2008.

2.4 PM-ISE References

- ISE-FS-200, Information Sharing Environment (ISE), *Functional Standard (FS), Suspicious Activity Reporting (SAR)*, Version 1.5, May 21, 2009.

EGuardian-580
UNCLASSIFIED//FOR OFFICIAL USE ONLY

3 Acronyms

(Same as in Volume 1)

Acronym	Definition
ABAC	Attribute Based Access Control
AFB	Air Force Base
AFOSI	Air Force Office of Special Investigations
AJAX	Asynchronous JavaScript and XML
ASA	Americas' Security Affairs
C&A	Certification and Accreditation
CJIS	Criminal Justice Information Services
CoE	Corps of Engineers
DAC	Discretionary Access Control
DBMS	Database Management System
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DOJ	Department of Justice
ERWin	(registered trademark)
FBI	Federal Bureau of Investigation
FL	Florida
FTTTF	Foreign Terrorist Tracking Task Force
GUI	Graphical User Interface
GW	Global Watch
HD	Homeland Defense
HD & ASA	Homeland Defense and Americas' Security Affairs
HSPD	Homeland Security Presidential Directive
HTTPS	HyperText Transfer Protocol, Secure
I2MS	Investigative Information Management System
I&A	Identification and Authentication
IEPD	Information Exchange Package Documentation
ISSO	Information System Security Officer
JDBC	Java DB Connection
JPA	Java Persistence API
JSF	Java Server Faces
JSP	Java Server pages
JTF	Joint Task Force
JTTF	Joint Terrorist Task Force
LEO	Law Enforcement Online
MD	Maryland
MDR	Metadata Registry
MTAC	Multi-Threat Alert Center
M-V-C	Model, View, Controller (form of architecture)
NCIS	Naval Criminal Investigative Service
NCR	National Capital Region
NCTC	National Counterterrorism Center
NGB	National Guard Bureau
NIACAP	National Information Assurance Certification and Accreditation Process

EGuardian-581

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Acronym	Definition
NIEM	National Information Exchange Model
NORTHCOM	Northern Command; Informal reference to USNORTHCOM
NSI	National SAR Initiative
NSI-EE	National SAR Initiative and Evaluation Environment
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OASD	Office of the Assistant Secretary of Defense
OASIS	Organization for the Advancement of Structured Information Standards
ORI	Originating Agency Identifier
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
PFFA	Pentagon Force Protection Agency
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Program Manager
PM-ISE	Program Manager for Information Sharing Environment
PMO	Program Management Office
RBAC	Role-based access control
S/L/T	State/Local/Tribal
SAN	Storage Area Network
SAR	Suspicious Activity Reporting
SIG	Special Interest Group
SPM	Security Policy Manual
SSL	Secure Socket Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
T3G	TALON System Termination and Transition Group
TALON	Threat and Location Observation Notice
TISS	Tactical Information Sharing System
TMU	Threat Monitoring Unit
TRB	Technical Review Board
U-Core	Universal Core
USA	US Army
USORG	US Organization
USPER	US Person
VA	Virginia
XML	Extensible Mark-up Language
XSD	XML Schema Definition

EGuardian-582

UNCLASSIFIED//FOR OFFICIAL USE ONLY

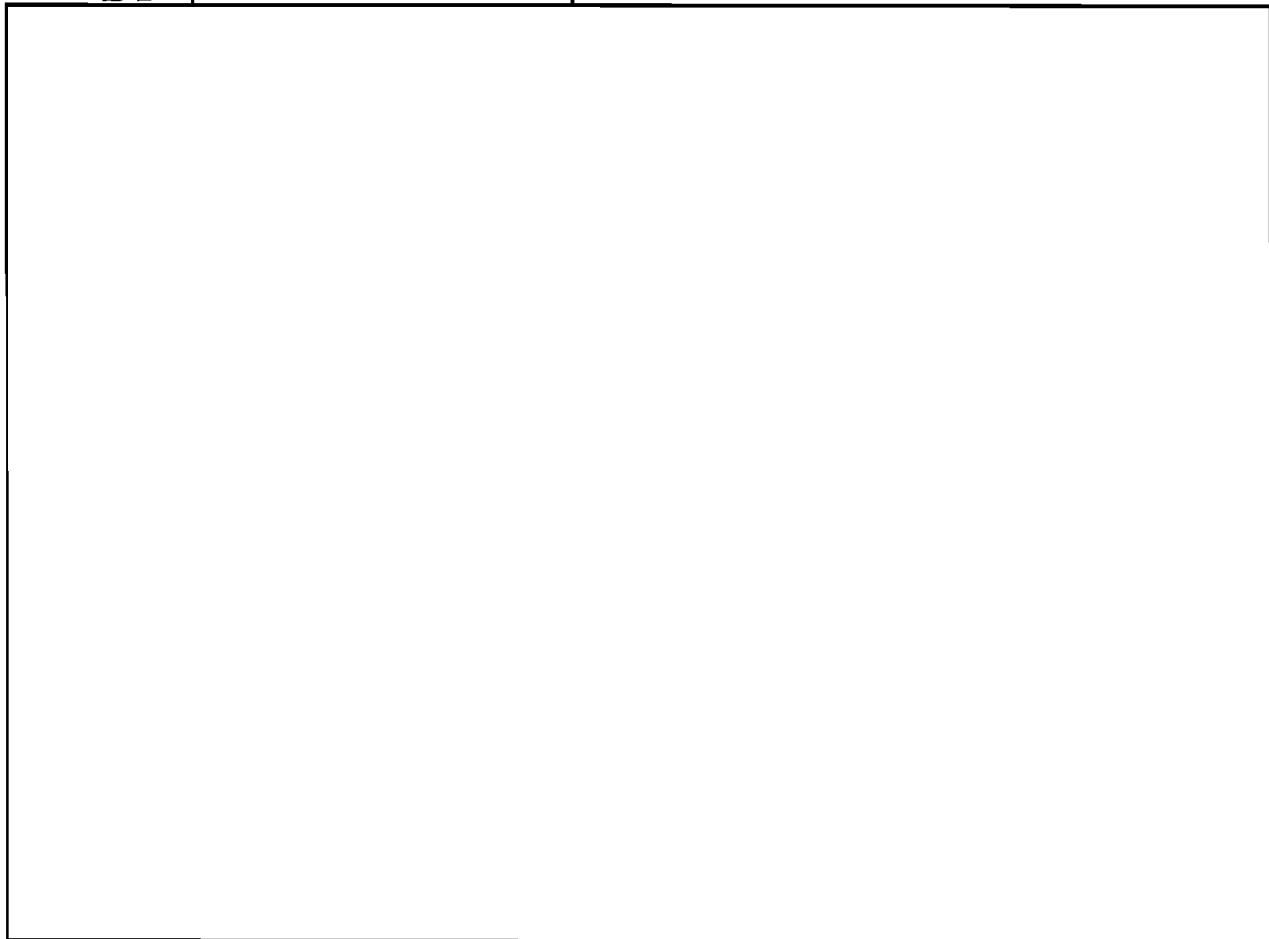
Appendix E eGuardian System and Software Description

All of the information in this section is based on several slides provided by the eGuardian PM, answers to specific questions, the SSP.

E.1 General Overview

The eGuardian system has been developed based on the Guardian requirements but is an unclassified system which allows input and search for any authorized US law enforcement entity (federal, state, local, or tribal). The FBI Threat Monitoring Unit (TMU) is the official interface with the user community for authorizing users and for determining requirements and priority of requirements.¹

E-2



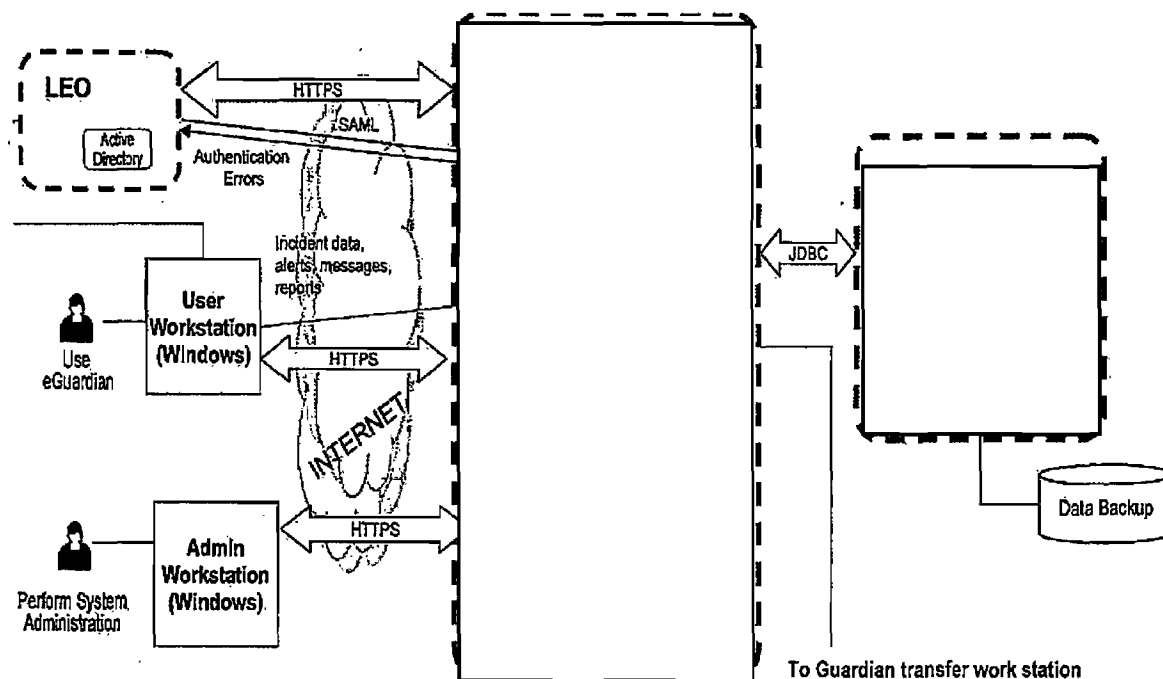
b6 per FBI
b7C
b7E

¹ Email from [redacted] 7/6/2009 3:56 pm, answering questions.

² Slides page 14.

E.3 Software Architecture and Design

The diagram below in figure E.2 illustrates (page 10) the software design. There is a secure three tier architecture: 1) the user workstation, [REDACTED] and 3) database server based upon Oracle Database Server (DBMS) version 10g, Oracle Virtual Private Database, and Oracle DataGuard for synchronizing standby database with the primary database in the DBMS computer.



b7E

(caption Figure E.2 Software Architecture)

Law Enforcement Online (LEO) server, which manages initial user accesses [REDACTED]

Communication between the workstation and the Web application server is HTTPS, encrypted using Secure Socket Layer (SSL).³ Similarly communications between the Applications Server and Database servers is encrypted using SSL.⁴

The Modular Model-View-Controller Architecture is employed.⁵ This means that there is a split in the application into separate layers that run on different computers: the presentation/user interface (UI) (view)

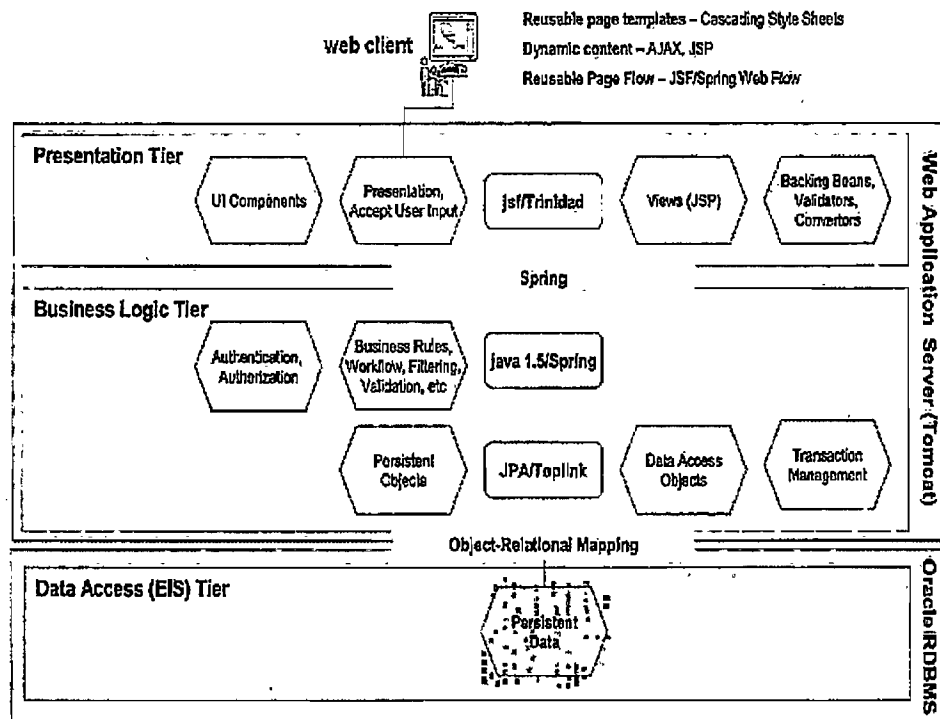
³ Slides page 10 shows HTTPS, and page 19 states that all communications are encrypted using SSL.

⁴ *Ibid.*

⁵ *Ibid.*

(called Presentation Tier below), business logic (controller) called business Logic Tier, and Data Access (model) call Data Access Tier.

The data access is supported by the DBMS computers. The functions in each tier are illustrated in the Figure E.3 below and described in the following paragraphs.



b7E per FBI

(caption Figure E.3 Application Architecture)

Users: there are two types of users: 1) [redacted] view history, and create reports; and 2) System administrators who edit incidents, delete incidents, refer incidents to Guardian, manage messages, and manage alerts. Both enter the system via LEO.

The Web Client (browser) uses Reusable page templates using Cascading Style Sheets; dynamic content using Asynchronous JavaScript and XML (AJAX), JavaServer pages (JSP); and Reusable Page Flow using JSP/Spring Web Flow.⁶

The Application Server is divided into two part or tiers, the Presentation Tier and the Business Logic Tier. Looking at the **Presentation Tier** first, Java Server Faces (JSF) using jsf/ Trinidad is the central controlling software for this Tier. It separates presentation from business function, manage objects (such as validators, convertors, and listeners) included on the JSP page. This tier includes user interface (UI) components, presentation and accept user input (SAR records or query input), Views implemented using

⁶ Slides page 11.

JSP, and Backing Beans,⁷ Validators, and Convertors. The bridge between the Presentation Tier and the Business Logic Tier is Spring.⁸

The Business Tier is controlled by Java 1.6/Spring and the JPA/EclipseLink. This tier includes the Authentication Service which provides the security access control for the eGuardian application. The Authentication Service employs SAML token-based Authentication with Role-based access control (RBAC) to authorize access. In addition this tier includes the business rules, flexible workflow, filtering, validation, etc. The interface to the database is also contained in this Tier, where the Java Persistence API (JPA) using JPA/EclipseLink provides state and data persistence. It supports persistent Objects, Data Access Objects, and Transaction Management⁹ In the business logic tier.

The connection with the Oracle BDMS is by Java DB Connection (JDBC). This interface to the Data Access Tier includes Object-Relational Mapping performed by JPA (see above).

Data Access (EIS) Tier consists of the data update and access using Oracle DBMS features. The application server software creates SQL statements for all update and query functions. Oracle Virtual Private Database is used for Data Segmentation for separation of draft (not shared) data.

Reports Currently there are only two canned reports available. The plan is that once there are 1) sufficient data and 2) user report requirements defined (through TMU), a rich set of canned and dynamic reports will be implemented. Currently the two reports are implemented using JasperReports and iReport.

Import/Export

Data exchange is based on the XML-based Information Exchange Package Documentation (IEPD) National Information Exchange Model (NIEM) formats.¹⁰ Currently the only such exchange is with the Guardian system. The XML Schema Definition (XSD)¹¹ is used for import/export. Data communications uses HTTPS/SSL encrypted communications.¹²

E.4 System Design

The user workstation is MicroSoft Windows using Internet Explorer and Adobe Reader.

There are four redundant Application Server systems are SunFire v20 using SUN Solaris as their operating system. Plans call for the additional Administrative Server and Report Server in the future which would use SunFire T2000 systems.

The two (redundant) Oracle Database Server systems (primary and standby) are SunFire 280r systems using SUN Solaris. Attached via Network switch both Sunfire 280r are two EMC CX-600 Storage Area

⁷ A backing bean defines UI component properties, each of which is bound to either a component's value or a component instance. A backing bean can also define methods that perform functions associated with a component, including validation, event handling, and navigation processing.

(<http://java.sun.com/j2ee/1.4/docs/tutorial/doc/JSFIntro8.html>) viewed on 7/20/2009.

⁸ Slides page 11.

⁹ *Ibid.*

¹⁰ The Information Exchange Package Documentation (IEPD) Clearinghouse provides information on a variety of IEPDs that have been submitted by individuals and organizations who have implemented the Global Justice XML Data Model (Global JXDM) and the National Information Exchange Model (NIEM).

(<http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm>) viewed 7/20/2009.

¹¹ The XML Schema definition language (XSD) enables you to define the structure and data types for XML documents. An XML Schema defines the elements, attributes, and data types that conform to the World Wide Web Consortium (W3C) XML Schema Part 1: Structures Recommendation for the XML Schema Definition Language (<http://www.w3.org/2001/XMLSchema>) viewed 6/28/2009.

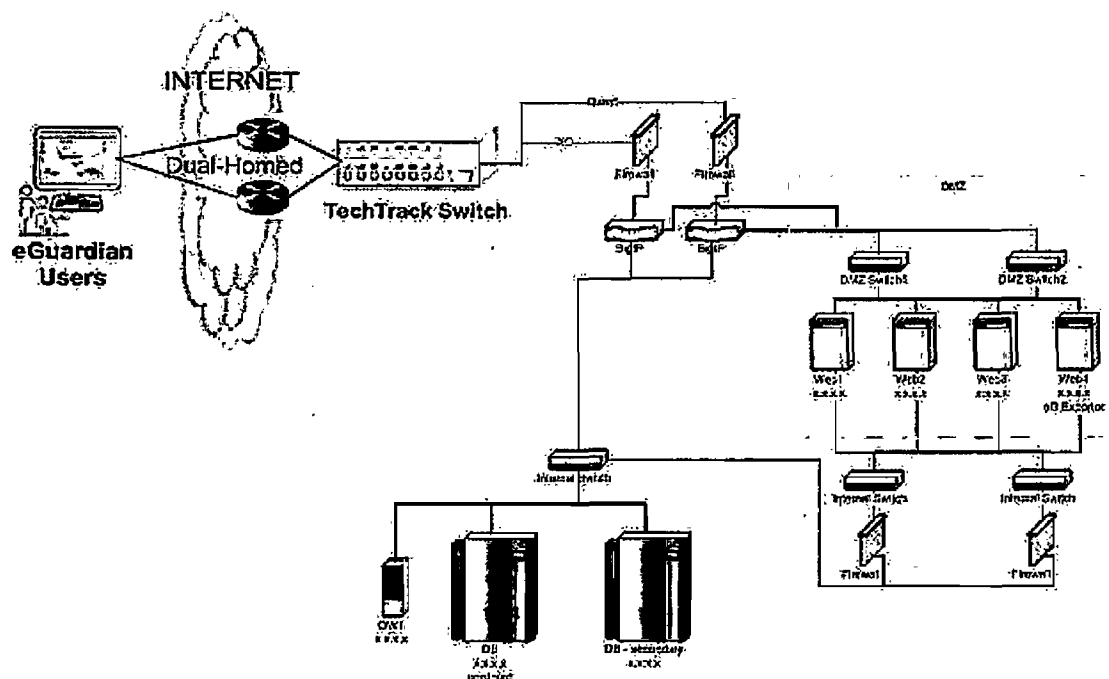
¹² Slides page 9.

Networks (SANs) for data storage with attached Quantum 1800 Tape Library (for making backup copies of the data).

Applications Servers are a cluster controlled by L5 BIG-IP load balancers. Network switches are Cisco 3524. Firewalls are Sidewinder.

E.5 Network Design

The network design as shown in figure E.4 below.



(caption: Figure E.4 eGuardian Network design)

Just inside the firewalls separating the eGuardian network configuration from Techtrack, there is monitoring for intrusion detection.

E.6 Development Environment

The Eclipse tool is used as the software development environment. It provides the JAVA editor and compiler; it also allows the developer to integrate directed into conveniently integrate new code into the TOMCAT Apache web server environment.

eGuardian is planning to adopt and use the full Rational suite of development tools for requirements, design documentation, development, configuration management, and testing. Currently, several tools are used (e.g., the CVS product is used for software configuration).

E.6.1 Testing Procedures

The eGuardian does not employ independent testing in the development process. However, early in the project a test engineer was brought on to establish strong test procedure practices. For example:

- With each spiral release, the formal test plan includes tests that verify each requirements being met by that release

Test Procedures consist of Functional and System test cases. Each test case lists: Requirements Tested complete with prerequisite conditions and step-by-step procedures. Pass/Fail as applicable is verified and annotated by a witness.¹³

As part of the testing of the initial and subsequent releases, each failed test is determined (with tester input) to be in one of several categories, e.g.:

- Critical (must be fixed before release),
- Reduced operational capability (should be fixed before release)
- Work around exists (should be fixed but there is a work around, which can be addressed with training)
- No reduced capability (inconvenience [suboptimal operation] only, should be addressed in training)
- Nice to have but does not reduce capability (can proceed with release but must be fixed before FOC)

For defect tracking eGuardian developers currently use "trac" software described at (<http://trac.edgewall.org/>).¹⁴ eGuardian is in the process of migrating to Rational for configuration control.¹⁵

E.6.3 Configuration Control

For Source-code control eGuardian uses CVS.¹⁶ eGuardian is in the process of migrating to Rational for configuration control.

E.7 Operational Considerations

E.7.1 Configuration Control

Next version is v 1.2 and will contain the following features.

1. Guardian-to-eGuardian Messaging - When incident are received, worked, transferred, and closed in Guardian, status messages will be sent down to eGuardian that contain the event, and contact information. These messages will be associated with the respective incident in eGuardian for viewing.
2. Enhanced Notification - Receive email notifications based on various events. For example, send me an email any time an incident is referred that originated with any DoD organization.
3. Import Service - Provide the ability for external organizations, such as the PMISE, to send (instead of type) incidents into eGuardian. Incidents will be accepted in XML format, using the NIEM XML schema. Incidents can also be exported into the NIEM XML.

¹³ Slides page 21

¹⁴ Email from [redacted] 6/29/2009 at 3:43 pm.

¹⁵ *Ibid.*

¹⁶ *Ibid.*

b6 per FBI
b7C

E.7.2 Failover Scheme

The multiple applications servers (cluster) serve two purposes. For performance their use is controlled by the load balancers (there are two load balancers for redundancy-only one in operation at any given time). The load balancers are configured such that once a user session is assigned to a particular application server, that use continues to use that applications throughout the session or until the application server fails. In that event, the user's session is ended and the user must log on again through LEO and be assigned to a different application servers. Any unsaved information would be lost at that point.¹⁷

E.7.3 Disaster Recovery



E.8 Evaluation Discussion

Scalability

Here scalability shall mean the inherent in the architecture of the system and software is the ability to easily increase the capacity of the system (e.g., adding or upgrading hardware) to accommodated large numbers of users, e.g., 10,000.

b7E per FBI

[REDACTED] MITRE has not performed an performance analysis of the database schema to determine if it is optimized for retrieval efficiency. However, the structure of the system architecture lends itself to increasing capacity through additional of application servers and database servers.

Reliability

According to the ISO 9126 Quality Characteristics, reliability includes maturity (few bugs), recoverability, and fault-tolerance.¹⁹ We are concerned about maturity and recoverability.



Maintainability

According to the ISO 9126 Quality Characteristics, maintainability includes stability, analyzability, changeability, and testability.²⁰

There was insufficient time to evaluate the maintainability. Because the design documentation was not current, the only way to judge the maintainability was to do a code review, which is recommended. Suggest that DoD support assistance to FBI in updating the design documentation for eGuardian.

¹⁷ From discussion with [REDACTED] on 07/07/2009.

¹⁸ *Ibid.*

¹⁹ Rawashdeh, Adnam and Bassem Matakah, Journal of Computer Science 2(4): 373-381,2006, A New Software Quality Model for Evaluating COTS Components.

²⁰ *Ibid.*

b6 per FBI
b7C

Appendix F eGuardian Net Centric Features Evaluation

It is the Net Centric vision of DoD "To function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing:

- A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise.
- An available and protected network infrastructure (the GIG [Global Information Grid]) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.²¹

Net-centricity is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and warriors to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization. In essence, Net-centricity translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

To support this vision and concept, DoD has defined its Information Enterprise Architecture, concepts and implementation guidance for data and services, and technical architectures containing interoperable standards.

[REDACTED] were assessment using DoD's Net-Centric Checklist. This are summarized in the next section which is followed by the checklist for Data, Services, Information Assurance, and Transport.

b7E per FBI

In all of the tables that follow the follow terms are used:

Yes – Meets the requirement well.

No – Does not meet the requirements at all.

Partial – Meets parts of the requirements, or currently has plans to meet the requirement in the near future.

N/A – [REDACTED]

UNK – Unknown, the information was not available for review. For example, The Evaluation team did not request the TechTrack SSP where many of the network, configuration management, security incident response, details are contained.

F.1 Summary

The following is a summary table of the four key components of DoD's Net-Centric Checklist.

²¹ Department of Defense, Office of the Chief Information Officer, *Information Enterprise Architecture*, Version 1.1, May 2009

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DoD Reference: Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII) Department of Defense Chief Information Officer

The table below reflects a rough cut at determining whether the DoD's Net-Centric Standards for *DoD Net-Centric Data Strategy Overall* are met. Additional net-centric analysis provided in this document break down these components by specific design tenets and rationale.

No.	Topic	Rationale for Check Item		Meets DoD Requirement (Y, N, Partial)	Comments
1.	Data	The <i>DoD Net-Centric Data Strategy</i> is a key enabler of the Department's transformation by establishing the foundation for managing the Department's data in a net-centric environment. Key attributes of the Strategy include: 1. Ensuring data are visible, accessible, understandable, and trustable when needed and where needed to accelerate decision-making. 2. "Tagging" of data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery by known and unanticipated users in the Enterprise. 3. Posting of data to shared spaces for users to access except when limited by security, policy, or regulations.		Partial	3. All required security, privacy, and policy, requirements are adhered to.
2.	Services	Services provide an environment that enables the rapid development and deployment of services, with well-defined, realizable capabilities that can be used with other services to provide a range of simple and complex functions.		Partial	

b7E per FFI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
3.	IA/ Security	The Information Assurance (IA) and security measures (IAS) CESs are a framework and family of services that provide a foundation to implement uniform, consistent, and effective IA. The IAS Core Enterprise Services contribute to, but are not sufficient to ensure the security level of each service. They are invoked as needed by service providers and users to satisfy business and policy requirements and reduce cost. Information Assurance is defined as measures taken to protect and defend our information and information systems to ensure Confidentiality, Integrity, Availability, and Accountability, extended to restoration with protect, detect, monitor, and react capabilities.		Partial	
4.	Transport	The Transport Infrastructure is a foundation for Net-Centric transformation in DoD and the Intelligence Community (IC). To realize the vision of a Global Information Grid, ASD/NII has called for a dependable, reliable, and ubiquitous network that eliminates stovepipes and responds to the dynamics of the operational scenario— <i>bringing Power to the Edge</i>. To construct the Transport Infrastructure DoD will: 1. Follow the Internet Model 2. Create the GIG from smaller component building blocks 3. Design with interoperability, evolvability, and simplicity in mind Questions in this category aid in developing an understanding of the general philosophy used in designing the system under assessment. These questions are based on the belief that wherever possible systems should follow the "Internet model" with the goal of becoming "plug and play" building blocks of the Global Information Grid. The design tenet questions test to this ideal, but should not be looked at as qualifying or disqualifying gates.		N/A	

DUE per rEI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

F.2 Data

The *DoD Net-Centric Data Strategy* is a key enabler of the Department's transformation by establishing the foundation for managing the Department's data in a net-centric environment. Key attributes of the Strategy include:

- Ensuring data are visible, accessible, understandable, and trustable when needed and where needed to accelerate decision-making.
- "Tagging" of data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery by known and unanticipated users in the Enterprise.
- Posting of data to shared spaces for users to access except when limited by security, policy, or regulations.

The table below reflects a rough cut at determining whether the DoD's Net-Centric Standards for *DoD Net-Centric Data Strategy Overall* and *specific* design tenets are met.

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
A	<i>DoD Net-Centric Data Strategy</i>				
A.1	Describe how the system is aligned with the <i>DoD Net-Centric Data Strategy</i> . 1.Explain how the system "posts data before processing" (data available on the net as soon as it is created/acquired). 2. If not, when is it programmed to be aligned? 3.What controls are in place to ensure processes encourage the posting of data for activities to be executed?			Y	1.Data are/is available to the Law Enforcement community as soon as it is approved for sharing by the DoD Information Flow policy. 2. N/A 3. PM-ISE and DoD SAR Policy is the only form of "encouragement."
B	<i>Make data visible</i>				
B.1	Does the system provide discovery metadata, in	Users and applications will migrate from maintaining	eGuardian briefings	Partial	This will be accomplished for DoD by, e.g., DoD

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
	accordance with the <i>DoD Discovery Metadata Standard</i> (DDMS), for all data posted to shared spaces?	private data (e.g., data kept within system specific storage) to making data available in community- and Enterprise-shared spaces (e.g., servers and services available on the Internet). Data will migrate from being maintained in private data stores alone, to being made available in community and Enterprise shared spaces.			registering the SAR data in the Metadata Registry. Otherwise data is discoverable (searchable) by the users of eGuardian and systems with which it shares.
B.2	Is all of the data that can and should be shared externally beyond the programmatic bounds of your system visible (i.e., advertised) to all potential consumers of the data?	identify if the application is making use of Web services to expose its data.		Y	eGuardian is a web based system, accessible if an account is granted.
B.3	Describe how the system is making its data assets visible to consumers.	whether a consumer needs to know about a data asset and establish a point-to-point connection, or whether the data asset be "discovered."		Partial	The user can search for SARs in multiple ways. If a SAR is put in a user's favorites then that user will get updates on that SAR. Soon the user will be able to put in a key word tag and have SARs pushed to him/her based on that input.
B.4	Describe how consumers are able to locate the data assets available from your system.	whether a consumer needs to know about a data asset and establish a point-to-point connection, or whether the data asset be "discovered."		Partial	The user may have to search for certain SARs by geography, key word etc. However the user will have a "key word" alerts capability in the future that will push the SARs automatically to him or her.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
B.5	Describe how the system is making use of Web service standards (e.g., SOAP [Simple Object Access Protocol], WSDL [Web Services Description Language], UDDI [Universal Description, Discovery and Integration]) to make its data assets visible.	Question will elicit whether the program is taking advantage of some of the open standards for Web services. (Also referenced in Net Centric Operations and Warfare – Reference Model)	eGuardian Slides	Y	
B.6	Describe any subscribe/notify mechanisms for the visible data assets available within the program that alert users and other applications when data has been created or updated.	Question will elicit whether a consumer can be notified when data assets change.		Partial	In the future, users will be able to set alerts to be notified of updates to particular SARs or SAR areas.
B.7	Describe where potential consumers can go to become aware of the data assets being made visible by your program.	Question should elicit how the program's data is being advertised to potential consumers.	PM-ISE documents NCES Documents	Partial	For DoD users, this will be accomplished by the DoD registering the SAR data in its Metadata Registry. Otherwise by learning about the SAR sharing program PM-ISE.
B.8	Describe how the program provides dynamic, flexible, and threat tailorable solutions for exchanging data assets between different security domains (i.e., cross-domain) with flexibility to accommodate new operational needs with minimal impact on system and mission performance.	DoD 8500 series, DCID 6/3		Partial	There is only one cross domain exchange of SAR data [redacted] [redacted] [redacted] used by J1111Fs and the Intelligence Community.
C	<i>Make data accessible</i>				
C.1	Is all of the data that can and should be shared externally	Describe for each visible data asset what the data		Y	

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
	beyond the programmatic bounds of your program accessible to all potential consumers of the data with sufficient access permissions and without any additional programming effort?	consumer needs to access the data (e.g., an application client, a Web portal, access to a Web service, access to a shared data storage area, an XML (eXtensible Markup Language) schema/parser, etc.).			SAR data with the entire law enforcement community, federal (including DoD), state, local, and tribal entities. The access permissions are consistent with the community's current capabilities.
C.2	Are there any limitations for the client appliance (e.g., workstation, desktop, laptop, PDA [personal digital assistant]) to access your data assets?	Question will elicit whether the program is client neutral and supports standard presentation protocols.	eGuardian Slides and experience of author.	Y	Client software is browser only, with no special requirements.
C.3	Has the program explicitly identified the potential universe of consumers of that data? (local, COI, enterprise)			Y	User are Federal, State, Local, Tribal law enforcement and Intelligence Community.
C.4	Describe the program's architecture and the data separation from the presentation and business logic.	Question will elicit whether the program is an n-tier architecture where the data has been isolated from the business logic.		Y	Web application architecture using Model-View-Controller concept
C.5	Describe the security mechanisms used to restrict access to specific, visible data assets. Are there any mechanisms in place to protect the data in transit to the consumer?	Question will elicit whether appropriate security has been placed on data assets.		Y	Role based Access Control in conjunction with Data Segmentation and Oracle Virtual Private Databases. HTTPS/SSL used for all internet transfers.
C.6	Describe how the visible data assets are made available to other users outside the Community of Interest with a need for the data.	Question should help the assessor determine how easily the data is accessible.		Y	

..7E per FBI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
C.7	Describe the common design patterns employed in the program that aid in the accessibility of data assets.	Question will elicit whether the program is making use of design patterns to simplify and standardize how data assets are accessed.		Y	The access control is role based. XML exchange standards are used.
C.8	Describe the use within the program of the following design patterns: • Request-Response • Publish-Subscribe • Transactional or Read-Only • Synchronous or Asynchronous • Model-View-Controller	Question will elicit more detailed discussion than the previous question. However, the program will not necessarily employ all of these patterns.		Partial	Model-View-Controller design/architecture is implemented. In the future with improved alert capability, the system may use Request-Response, or Publish-Subscribe. There are plans to implement MQ for sharing in the PM-ISE arena, MQ is an asynchronous messaging capability
C.9	Describe how the program provides assurance that there is timely and reliable access to data assets anytime, anywhere for authorized users/entities.	DoD 8500 series, DCID 6/3. Integrity is a core information assurance (IA) function, and is necessary to provide confidence in data received		Y	
D	<i>Make data understandable</i>				
D.1	Is all of the data that can and should be shared externally beyond the programmatic bounds of your program sufficiently documented and understandable that any potential consumer can comprehend the structural and semantic meaning to determine how they may use it appropriately?	Metadata tagging enables users to discover the data for retrieval. The assessor should assess whether sufficient use of metadata is being made.		Partial	

LOE per FBI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
	Describe how the program tags data with discovery metadata.				
D.2	Explain how the program is making use of the DoD Metadata Registry and Clearinghouse.	whether discovery metadata is being generated that is compliant with the DoD Discovery Metadata Specification.		Partial	For DoD users, this will be accomplished by DoD registering the SAR data in the Metadata Registry. Access to this registry is unknown
D.3	Describe the source of all XML elements. • Has the DoD Metadata Registry been used whenever possible? • Have newly defined XML elements been registered with the Registry?	whether the program is making use of existing, registered data elements from the Registry.		Partial	The DoD Metadata registry may be very new.
D.4	Describe any data schemas or standards being applied in the program.	whether the program is using XML Schemas, DTDs [Document Type Definition]		Y	OASIS standards, XSD and NIEM are used.
D.5	Describe any automated mechanisms that are available for data mediation/translation (e.g., XSL [eXtensible Stylesheet Language], XSD [XML Schema Definition]).	data translation capabilities that are available.		Y	XSD is used.
E	<i>Make data trustable</i>				
E.1	Can all potential consumers of all of the data available from your program determine the data pedigree (i.e., derivation and quality), security level, and access control level of your data?	how a consumer can determine data asset quality.		Partial	Authors are included in the SAR record. There is no other quality information in the record. However, the purpose of SARs is to invoke investigations to validate and find relations to other intelligence.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
E.2	Describe for each visible data asset in the program whether the program is the authoritative data source.	whether any data assets are secondary sources.	eGuardian database schema analysis by MITRE.(name the document)	Partial	Authors are included in the data record. There are levels of approval required by the DoD Information Flow policy. Wide use of reference tables assure use of valid information such as Zip codes, city names, etc.
E.3	Describe what measures the program takes to ensure the integrity of the data (for internally used data, externally used data, and data that simply transits the program).		eGuardian Slides	Partial	Data in the system is protected as prescribed for its security level. All data in transit is encrypted appropriately. There are not integrity measure of data as it is used externally
F	<i>Make data interoperable</i>				
F.1	Does all of the data that can and should be shared externally beyond the programmatic bounds of your program have sufficient metadata descriptions and automated support to enable for mediation and translation of the data between interfaces? Describe any programming changes that would need to be made to the program if a new consumer of a visible data asset were identified.	whether new consumers can be added with no additional cost/effort or whether a new point-to-point interface needs to be established.	ISE-FS-200, ISE, Functional Standard (FS), Suspicious Activity Reporting (SAR), Version 1.5, May 21, 2009.	Y	Such data conforms to the PM-ISE standard for SAR data exchange.
F.2	Identify the published net-centric interoperability standards (e.g., DDMS) to which the program adheres.			N/A	
F.3	Describe the process a	identify programs that have		Y	Use the User Feedback

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
	consumer would follow to a) request changes in the format (syntax or semantic) of the visible data asset; b) report a problem with a data asset; or c) request additional data from the data provider.	thought through customer service and planned for accommodating changing consumer needs.			feature; raise the issue at the TMU SAR working group meeting; contact the eGuardian help desk (PM).
G	<i>Provide Data Management</i>				
G.1	Is there sufficient management of all of the data available through your program to adequately maintain and improve your data assets within a changing environment? Describe the effort associated with the program to define, develop, and maintain an ontology (i.e., schemas, thesauruses, vocabularies, key word lists, and taxonomies) that best reflects the community understanding of the "visible data assets."			Partial	 eGuardian database. The Schema has strong configuration control. The SAR record content is the subject of the PM-ISE and TMU.
G.2	Describe your processes for ensuring the usefulness and timely availability of all data assets associated with your program.			Partial	Customized work flows.
G.3	Describe the various data survivability scenarios considered in your program.	data survivability capability of the program and the consumer's experience as a result.		Y	Comprehensive auditing is performed and regularly reviewed. Daily partial backups and weekly total backups are made and kept at a different location.
H	<i>Responsive to user needs</i>				

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
H.1	Are perspectives of users, whether data consumers or data producers, incorporated into data approaches via continual feedback to ensure satisfaction?			Y	Yes through LEO and through the TMU user working group.
H.2	What tools, services, processes, and resources is the program providing to facilitate user feedback and program responsiveness with respect to data needs?	determine if the program is putting in place appropriate mechanisms to enable responsiveness to user data and application needs.		Y	There is a user feedback button built into the system for easy access. User feedback is monitored by staff and PM.
H.3	What metrics are being used to determine responsiveness to user data needs?	determine the program's ability to measure its responsiveness to user data and application needs.		N	None in place currently
H.4	What is the degree of collaboration with respect to data that is enabled and is occurring among the user community (ies) and the program developers?	assess the actual degree of visibility into ongoing user needs and the responsiveness and quality of interaction with respect to user data and application needs.		UNK	The Evaluation has been very interactive with the developer (PM) during the Pilot
H.5	What are measured/assessed trends over time with respect to the program's responsiveness to user data needs and degree of satisfaction towards meeting those needs?	determine the degree of program improvement in being responsive to user data and application needs over time.		Y	Substantial improvement in functionality (e.g., search) has been noted between the Interim Pilot Report and this Report.
H.6	What are the programs plans to enhance responsiveness to user data needs?	determine potential for improving future responsiveness to user data and applications needs.		Y	New features planned are directly responsive to previous user feedback.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

F.3 Services

Services provide an environment that enables the rapid development and deployment of services, with well-defined, realizable capabilities that can be used with other services to provide a range of simple and complex functions.

The table below reflects a rough cut at determining whether the DoD's Net-Centric Standards for *DoD Service Oriented Architecture Overall* and *specific design tenets* of the strategy are met.

No.	Topic	eGuardian Reference	Meets DoD Req.	Comments
A	<i>Service Oriented Architecture</i>			
A.1	Describe how the program will make its unique services/applications available to the GIG community.			The likely method will be through DoD systems that interface with eGuardian (e.g., I2MS). These interfaces have not been implemented.
B	<i>Open Architecture</i>			
B.1	Is the system architecture based on loosely-coupled interactions, enabling the internal components to map to well-defined external interfaces? Describe.	eGuardian Slides	Y	The system uses Model-View-Controller modular architecture.
B.2	Are Web services implemented by the program built using core standards as defined in		Y	Uses Apache Tomcat web Server, JAVA tools
C	<i>Scalability</i>			
C.1	What estimates of service usage have been developed (How many expected consumers? How many service invocations per hour (or per some appropriate unit of time)? What assumptions or empirical tests are these estimates based?		Y	8000 expected users, 3000 simultaneous users at worst case crisis mode. This information is based on survey of Services.
C.2	What performance analysis has been done to understand or predict the ability of the service to handle the expected load (e.g., number of enduser consumers or number of calling services)?		P	A simulation based performance test has been run for 500 users.
D	<i>Availability</i>			
D.1	Does the program have a continuity of operations plan? What is the plan for providing service during routine maintenance (hardware and software)? What is the plan for providing service during catastrophic		P	Plans are currently being formulated and a DR site is expected to be implemented in FY2010. The service has a low availability requirements so no provision is needed for routine maintenance.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	eGuardian Reference	Meets DoD Req.	Comments
	failures (e.g., massive outages of the power grid, physical destruction of the hosting facility)? Does the continuity of operations plan include procedures for finding, housing, and supporting the technical support staff during an emergency action?			Users are distributed in various DoD organizations. Therefore only system support staff are required to be provided for. Expect that arrangements will be made to share responsibilities such that there is minimal need for staff movement.
D.2	What threat scenarios have been considered in the planning?		UNK	
E	<i>Accommodate heterogeneity</i>			
E.1	How will the service adapt to delivering end-to-end capabilities over a range of bandwidths (from low bit-rate tactical communications to multi gigabit backbone service), environments (fixed and wireless), and end user devices (e.g., PDAs, laptops, workstations, mainframes)?		Y	All access is currently planned to be over the Internet or directly connected to DoD LE systems. No special planning is required.
E.2	Describe how the program will support delivery of capabilities to thin or browser-based clients, especially those that provide adaptability to a variety of disadvantaged 'edge' environments for end-users.		Y	The system only supports browser based clients.
F	<i>Decentralized operations and management</i>			
F.1	Does the service offering support a decentralized operational concept where other systems, services, or capabilities are providing key elements of the end-to-end net-centric solution?		Y	
F.2	Does the service offering depend on or use any other services provided by a different program or service provider? If so, explain how this works.		Y	
G	<i>Enterprise Service Management</i>			
G.1	Does the service provide instrumentation to enable the service provider to determine the current operational state and performance level of the service?		UNK	They use tools provided by the Web server and operating system. There are no service level agreements.

b7E per FEI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	eGuardian Reference	Meets DoD Req.	Comments
G.2	Will service management information, including performance metrics and problem/outage status information, be made available to consumers of the service as well as the service provider?		Y	This requirement should be included in the MOU.
G.3	What protocols and standards are used to collect and disseminate service management information, and in what format will it be made available (e.g., SNMP (Simple Network Management Protocol), XML, CIM (Common Information Model) – SNMP and XML are identified as mandated standards in Sections 2 and 3 of the JTA, Volume I. CIM is an emerging standard identified in paragraph 2.5.10a of the JTA, Volume II. CIM is also identified as a target standard in the NCOW Reference Model [v. 1.0]).		Y	NIEM for SAR, XSD, SAML, JDBC, JSF, JPA are used.
G.4	List and provide completed examples, including net-centric and NetOps elements/attributes, of all Service Level Agreements (SLA) negotiated by this service provider with others (e.g., transport layer programs, other service providers, consumers).			Should be included in the MOU with FBI.

F.4 Information Assurance

The Information Assurance (IA) and security measures (IAS) CESs are a framework and family of services that provide a foundation to implement uniform, consistent, and effective IA. The IAS Core Enterprise Services contribute to, but are not sufficient to ensure the security level of each service. They are invoked as needed by service providers and users to satisfy business and policy requirements and reduce cost. Information Assurance is defined as measures taken to protect and defend our information and information systems to ensure Confidentiality, Integrity, Availability, and Accountability, extended to restoration with protect, detect, monitor, and react capabilities.

The table below reflects a rough cut at determining whether the DoD's Net-Centric Standards for *DoD Net-Centric IA Strategy Overall* and *specific* design tenets of the strategy are met. If items are addressed in the Security Section, they are omitted here

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
A	<i>DoD Net-Centric IA Strategy Overall</i>				
A.1	Explain how the program is aligned with the DoD Net-Centric Information Assurance Strategy. If not, when is it programmed to be aligned?		eGuardian SSP, eGuardian slides	P	
B	<i>Net Centric IA Posture and Continuity of Operations</i>	Covered in 8500.2 chart.			
C	<i>Identify Management, Authentication and Privileges</i>	Covered in 8500.2 chart.			
D	<i>Mediate Security Assertions</i>	Covered in 8500.2 chart, except as below			
D.1	Does the program mediate security assertions (to pass security related information between systems, processes, and domains)? If yes, how does the program mediate security assertions? If no, explain.	whether the service application itself is used to implement XML-signature, XML-encryption, etc.	eGuardian SSP, eGuardian Slides	Y	
E	<i>Cross Security Domains Exchange</i>	Covered in 8500.2 chart			
F	<i>Encryption and HAIPE</i>				
F.1	Have program requirements for encryption been coordinated with the High-Assurance Internet Protocol Encryption (HAIPE) Working Group? If no, explain.		eGuardian SSP, eGuardian Slides	N	

b7D per FBI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

28

EGuardian-605

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
G	<i>Employment of Wireless Technologies</i>				
G.1	Do you (plan to) employ wireless technologies? If yes, which wireless technology and standards will be used?		eGuardian SSP (not mentioned)	N	Wireless communication is not currently contemplated.
G.2	What confidentiality level (public, sensitive, classified) applies to the data being transmitted via wireless technologies?			N/A	
H	<i>DoD 8500 series</i>	Covered in 8500.2 chart except as below.			
H.9	Does the system provide the capability to bind strongly the user/entity physical characteristics and attributes to their digital identity?		eGuardian SSP	N/A	
H.10	Does the system provide a means for authenticating all GIG entities and for verifying their access credentials are valid and active?		eGuardian SSP	N	Assume all GIG entities use PKI which is not supported.
H.11	Does the system provide the capability to manage access to the GIG information and resources based upon the GIG digital security policy as well as the entity's credentials, privileges, roles, and profile?		eGuardian SSP	N	
H.12	Does the system provide proactive measures to protect against known and new vulnerabilities to itself and the rest of the GIG?		eGuardian SSP	N/A	

b7L p e1 FE

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
H.13	Does the system provide a defensive capability that contains, recovers, restores, and reconstitutes itself or the GIG against incidents (e.g., failure, anomaly, attack, misuse, intrusion, etc)?		eGuardian SSP	N/A	
H.14	Does the system have an IA capability to provide timely, reliable access to processes and data even in the event of a denial of service attack?		eGuardian SSP	N	Currently access is only through the Internet and LEO.
H.15	Does the system have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability or procedures for performing unauthorized system operations?		eGuardian SSP	Y	
H.17	Does the system have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network to secure the information and this capability shall also be available for operations involving allied and coalition forces?		eGuardian SSP	Y	It uses HTTPS/SSL encryption with 128 bit keys. ²²
H.18	Has an information assurance, risk management program been		eGuardian SSP	Partial (Not sure)	Was in the Techtrack SSP.

b3F per EPT

²² Email, Wednesday, September 02, 2009 7:30 PM from Brian Schleser, CISSP, C|EH, Security, forwarded by [REDACTED]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

b6 per FBI
b7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY

No.	Topic	Rationale for Check Item	eGuardian Reference	Meets DoD Requirement (Y, N, Partial)	Comments
	developed?				
H.19	Is a Concept of Operations (CONOPS) & COOP program in place (i.e., documentation, training, testing, technical, and physical, etc.)?		eGuardian SSP	P	Found draft CONOP, no COOP document yet.
H.22	Does the system have requirements for handling coalition or multinational data?		eGuardian SSP	UNK	No currently to the Evaluation teams' knowledge
H.25	How will addressable IP devices be protected from denial of service attacks? What criteria do these devices have for availability?		eGuardian SSP	Y	
H.26	What measures are in place to protect against role or identity theft?		eGuardian SSP	Y	Same as for data protection.

b7E per FBI

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Appendix G eGuardian Privacy Evaluation

Results of Mapping of eGuardian Privacy Impact Assessment (PIA) to DoD PIA Template

17 July 2009

The table below presents the results of mapping the eGuardian Privacy Impact Assessment (PIA), which is posted at http://foia.fbi.gov/eguardian_threat.htm, to the DoD's PIA template, DD Form 2930, dated November 2008.

DoD PIA Template Section	Topic	eGuardian PIA Section where topic is addressed	Comments/Recommendations
1	PIA Required	1.0	
2a	Why is PIA being done	Introduction	
2b	Where is IT registered (DITPR or SPIRNET)	N/A	
2c	Unique identifier with OMB	N/A	
2d	SORN required?	6.0	
2d	SORN Identifier	N/A	
2e	OMB Control Number	N/A	
2f	Authority to collect information	2.2	
2g (1)	Purpose of information	Introduction, 1.1, 2.1	
2g (2)	Privacy Risks	2.3	
2h	With whom shared	4.0, 5.0	
2i	Individuals' objection	6.2	
2j	Individuals' consent	6.3	
2k	Information provided to individuals	6.1	
3a (1)	PII collected	1.1	The DoD form provides a list of types of PII with checkboxes for the respondent to use to indicate which of the types of PII are collected. The eGuardian PIA addresses what information will be collected in Section 1.1. However, the response in the eGuardian PIA is more general – it states that PII “to be collected will include all available identifiers regarding the subject of a report or incident, such as name, date and place of birth, unique identifying numbers, physical descriptions, and similar attributes.” You may want to take a look the list

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DoD PIA Template Section	Topic	eGuardian PIA Section where topic is addressed	Comments/Recommendations
			of PII attributes given on the DoD form and determine specifically which of those are collected for eGuardian and add that information to the eGuardian PIA.
3a (2)	Sources of PII	1.2	
3a (3)	Method of information collection	1.2	Section 1.2 of the eGuardian PIA states generally how information is collected, but does not specifically identify the collection method (e.g., face-to-face contact, paper format, etc.)
3a (4)	Why specific PII is collected	2.1	
3a (5)	Use of specific PII is collected	3.1	
3b	Is information from data aggregation	Not addressed	The eGuardian PIA does not specifically address data aggregation; it does discuss data mining in Section 3.2.
3c	Who will have PII access	8.1, 8.2	
3d (1)	How PII will be secured	Not addressed	The eGuardian PIA does not address physical controls.
3d (2)	Technical Controls	8.3, 8.9	Section 8.9 of the eGuardian PIA says that the computer software and hardware components are secured behind an accredited FBI security infrastructure. Specific information regarding the topics listed in the DoD PIA template (User Identification, Biometrics, Password, Firewall, IDS, VPN, Encryption, PKI Certificates, etc.) is not provided in the eGuardian PIA.
3d (3)	Administrative Controls	8.4, 8.5, 8.6	
3e	C&A required?	8.8	eGuardian PIA information is related to FBI certification and accreditation (C&A) process, which is not the same as the DoD C&A process
3f	How will handling at each stage of life cycle affect individuals' privacy	Not addressed specifically	The eGuardian PIA does not discuss this topic specifically. However, answers to questions in many sections of the eGuardian PIA provide the information that is needed to answer this specific question, e.g., information in Section 1 of the eGuardian PIA can be used to address the collection stage, information in Section 3 can be used to address the use stage, information in Section 3 can be used to address the retention stage, information in Section 8 can be used to address the processing stage, and information in Sections 4 and 5 can be used to address the disclosure stage. The eGuardian PIA does not contain information that can be used to discuss information handling practices for the destruction stage.
3g	Measures to reduce privacy risk	9.3	Section 9.3 of the eGuardian PIA discusses design choices that were made to enhance privacy. This is related to the topic of addressing identified privacy risks, although it is not an exact match.
3h	Measures to reduce privacy risk for new systems	N/A	

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Appendix H eGuardian Security Evaluation

- Not included at this time due to work agreements with the FBI.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

34

EGuardian-611