IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 8 Number 3 • Winter 2005/2006

Net-Centric Assured Information Sharing:

Moving Security to the Edge through Dynamic Certification & Accreditation

also inside—

- IA/CND Enterprise-wide Solutions Steering Group or ESSG
- IATAC Spotlight on Research and Education
- IA Events—6th Annual IEEE IA Workshop
- A Honeypot for the Exploration of Spammers' Behavior
- Taxonomy Development Methodology
- Quarterbacking Information Management: A Content Staging Overview

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

The IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the U.S. Government, DoD, or DDR&E. The mention of commercial products and/or services does not imply endorsement by the DoD or DDR&E.

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director:	Gene Tyler
Deputy Director:	Greg McClellan
Inquiry Services:	Peggy O'Connor

IAnewsletter Staff—

Creative Directors:	Christina P. McNemar Ahnie Jenkins
Art Director:	Bryn Farrar
Copy Editor:	Diane Ivone
Designers:	Dustin Hurt Steve Green Ricardo Real José Weeks Kathy Everett
Editorial Board:	Jim Peña Ronald Ritchey Tara Shea Gene Tyler

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/IA_newsletter.html and download an "Article Instructions" packet.

IAnewsletter Address Changes/Additions/Deletions

To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
3190 Fairview Park Drive
Falls Church, VA 22042

Phone:	703/289-5454
Fax:	703/289-5467
E-mail:	iatac@dtic.mil
URL:	http://iac.dtic.mil/iatac

Deadlines for future Issues—

Spring 2006	April 7, 2006
Cover design:	Dustin Hurt
Newsletter design:	Ahnie Jenkins

Distribution Statement A:

Approved for public release;
distribution is unlimited.

IATAC Chat

Gene Tyler, IATAC Director

This edition of our newsletter contains a fascinating article that describes how the DoD intends to accomplish the goals of net-centricity by implementing the DIACAP and a combined collection of supporting capabilities.

For years, the US Department of Defense (DoD) Information Technology Certification and Accreditation Process (DITSCAP) has been the process for certifying and accrediting Information Systems (IS). While the DITSCAP has served its primary function—verifying the security state of an individual DoD IS—it was never intended to support interoperability with enterprise systems and Information Assurance (IA) infrastructures and does not support common services past an individual system's requirements. The result is that each system owner develops his or her own requirements and solutions with no across-the-board standardization. This individualized process is no longer practical in an environment of so many linked, networked systems and is especially unrealistic as the DoD continues developing the Global Information Grid (GIG). The solution—a combined DoD program to revamp the Certification and Accreditation (C&A) process. This program includes the following:

- The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction, DODI 8501.XX
- The DIACAP Knowledge Base, a Web portal providing guidance on executing the DIACAP
- The Enterprise Mission Assurance Support System (eMASS), an integrated suite of government-owned management systems that will provide IA Program Management and C&A visibility
- The Vulnerability Assessment Management Service (VAMS), tools and technologies that will leverage the service-oriented aspects of the GIG

This edition of our newsletter contains a fascinating article that describes how the DoD intends to accomplish the goals of net-centricity by implementing the DIACAP and a combined collection of supporting capabilities.

In this edition of the IAnewsletter, you will also find the IATAC Spotlight on Research and Education, which focuses on the Air Force Institute of Technology (AFIT). This article is actually the first in a new series we at IATAC are pleased to debut, Information Assurance (IA) Education and Research at the Air Force Institute of Technology (AFIT), which will recur within the newsletter to inform our readers of AFIT's capabilities. Primarily, the series will focus on explaining the mission and the academic and research programs of AFIT's Center for Information Security Education and Research (CISER).

I certainly hope you enjoy reading this edition of the IAnewsletter. As always, if you have any questions, concerns, or ideas about the IAnewsletter, please let us know. We are here to support you, the professionals in the IA/IO community. ■

Gene Tyler

Net-Centric Assured Information Sharing—Moving Security to the Edge through Dynamic Certification & Accreditation

by Glenda Turner, Patrick Holley, Julie E. Mehan, and Michael Colon

Across the US Department of Defense (DoD), the goals of net-centricity are transforming the way in which Information Assurance (IA) must be achieved to facilitate assured information sharing, accelerate decision making, improve joint warfighting, and ensure the ability to dynamically exchange system-security credentials. Power to the Edge implies greatly enhanced peer-to-peer communications. "Security to the Edge" assumes the need to assure a system's security status and to provide security assertions precisely where interoperability and communications must occur. DoD soon-to-be published *Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*, combined with a suite of supporting capabilities, form an integrated program that proposes to address this emerging environment. DIACAP is generating increasing interest among its represented customers, DoD Components, and many other groups who are affiliated with developing the Global Information Grid (GIG).

The combined DoD program to re-engineer Certification & Accreditation (C&A) consists of the following:

- **The DIACAP Instruction** (DoDI 8510.xx)
- **A DIACAP Knowledge Service**, based in a Web portal, which provides comprehensive DIACAP implementation guidance
- **The Enterprise Mission Assurance Support System (eMASS)**, which seeks to provide IA Program Management and C&A visibility through an integrated suite of government-owned, relational-database management systems, based on Commercial-Off-The Shelf (COTS) products. These products are accessed through an associated Web interface that standardizes approaches for describing and collecting the required data for C&A and other core IA functions. eMASS enables IA managers and senior decision makers at all enterprise levels to comprehend more fully the scope and state of IA activities within the enterprise, which can assist in identifying IA requirements, developing policy, managing and training personnel, and making decisions concerning acquisition and IA resources and programming.
- **The Vulnerability Assessment Management Service (VAMS)** is designed to leverage the service-oriented aspects of the GIG by using state-of-the-art tools and technologies while strongly adhering to commercial and government IA best practices. VAMS is a data-consolidation utility. VAMS gathers IA information specific to a system or group of systems from various sources and correspondingly re-packages this information into a common, consolidated representation of an IA posture. VAMS is not intended to replace existing IA assessment products; rather, it is a supplementary collaboration utility for organizing and analyzing, in a more centralized manner, the data collected by distributed components.

Background

While C&A has long been considered an accepted, systematic means of addressing IA across the life cycle of Information Technology (IT), existing processes are no longer sufficiently flexible to address security information sharing in the GIG. In response to these emerging IA requirements, DoD developed a suite of IA policies that will accommodate the legal requirements surrounding IA, C&A, and the dynamic nature of the GIG.

In 2002, the following DoD policy set was cancelled:

- Department of Defense Directive (DoDD) 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems
- DoDD 5200.28-M, Automated Information System Security Manual Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems
- DoDD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria

These documents were superceded by a new set consisting initially of DoDD 8500.1, Information Assurance, and DoD Instruction (DoDI) 8500.2, Information

Assurance (IA) Implementation. This new document set adopted new concepts—Mission Assurance Category (MAC), Confidentiality Level, IA Controls, and Robustness—as follows:

- DoDD 8500.1, Information Assurance, establishes how DoD will describe the operational value of information in terms of confidentiality, availability, and integrity. It establishes three MACs that establish availability and integrity levels and three Confidentiality Levels relative to information classification, sensitivity, and need-to-know status.

- DoDI 8500.2 combines MACs and Confidentiality Levels with consensus or community-based best security practices, general threat information, federal and DoD policy requirements, and enterprise operational and technical considerations (*e.g.*, interoperability with specific services or supporting IA infrastructures) in a graded or banded risk model. The model establishes baseline IA requirements for all combinations of MACs and Confidentiality Levels in the form of IA Controls.

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

DITSCAP, the existing DoD C&A process, is based on the concept of verifying the security state of an individual DoD information system. Under the requirements of the DITSCAP, each information system determines its IA requirements and solutions independent of the larger environment in which it must operate, which results in tremendous variability in both process and outcome across DoD. Systems inhabiting or targeting the same environment may use very different approaches to identify and implement requirements, with significant variances in time, cost, and outcome. The DITSCAP does not require or support interoperability with enterprise systems and IA infrastructures, inheritance of IA services from the operating environment, or support to common services (beyond each individual system's needs). Essentially, each system develops its requirements and solutions in a vacuum without an enterprise "norm" or concept of adequacy. This results in a random mix of hardened and exposed systems. The vulnerabilities of exposed systems dilute the IA investments of hardened systems. Similarly, exposed systems may be unaware of and unable to take advantage of the localized IA services of hardened systems.

As expressed under the DITSCAP, the system-security status is heavily focused on documents. The primary documentation is the System Security Authorization Agreement (SSAA), in which each author independently decides how to describe requirements and solutions, what requirements and solutions apply, how to implement solutions, how to test, and how to assess risk. A lack of standardization in execution and terminology means that security documentation cannot easily be compared or analyzed across multiple system environments. Because the DITSCAP C&A cycle is three years, there can be no assurance that security information is current. And the DITSCAP process may be more expensive than is warranted by system-security requirements.

The End of the Isolated C&A Process

This type of isolated, platform-centric C&A process is no longer viable in an environment in which systems are evolving from discrete networked entities to nodes in the network. "These collections of entities will ultimately become dynamically reconfigurable packs, swarms, or other organizations of highly specialized components that work together like the cells of our bodies. As such, they will be able to be far more discriminating and precise in the effects they cause. They will become less mechanical and more organic, less engineered and more 'grown.'" [1] (See Figure 1.)

Change is Essential

In a net-centric environment, the concept of security based on the characteristics of individual systems becomes increasingly complex, "because it is impossible to reduce the overall behavior of the system to a set of properties

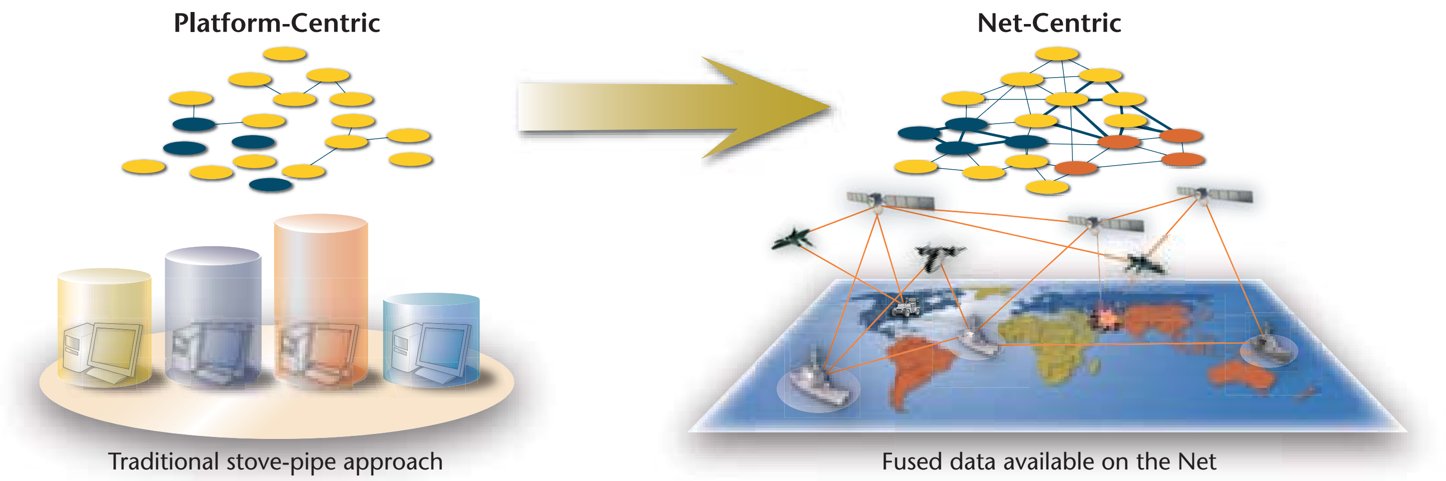

Platform-Centric
Net-Centric
Traditional stove-pipe approach
Fused data available on the Net

Figure 1. Platform-Centric to Net-Centric

characterizing the individual components. Interaction (between systems) is able to produce properties at the collective level that are simply not present when the components are considered individually." [2] Typically, complex systems must adapt their characteristics, including their security characteristics, in concert with the dynamics of the overall environment in which they operate.

The result is an intricate, self-organizing information network that might be described as a grid of connections—the GIG. The GIG is a net-centric environment. It provides an end-to-end set of information services, associated processes, and people to manage and provide the right information to the right user at the right time with appropriate protection across all DoD warfighting, intelligence, and business domains. The GIG assumes "service assurance," the guarantee that available system resources, services, and information are accessible, properly protected, and rapidly delivered when and where they are needed in the required form. Three derived "assurances," *Assured System and Network Availability, Assured Information Protection,* and *Assured Information Delivery,* are all required to achieve and sustain service assurance. The method of implementing service assurance in a net-centric environment is to establish operational thresholds and document expectations between enterprise services, resource providers, and consumers through Service Level Agreements (SLAs). The method of verifying and asserting that security assurance for DoD information systems is C&A. Consequently, the role of C&A assumes even greater importance within the net-centric environment, and the change to a more dynamic, net-centric C&A is essential.

Change Will be Difficult

Simply defined, change is the adoption of new behaviors or practices. To perform differently and adjust to change in an environment requires new learning (skills, knowledge, capabilities, and attitudes). Long-term change has four characteristics:

- **Scale**—The change affects the entire organization.
- **Magnitude**—The change requires significant transformations of the status quo.
- **Duration**—The change lasts for a significant period of time.
- **Substance**—The change is of strategic importance.

Change of this magnitude represents a "rapid and fundamental shift in the basic circumstances of the organization and requires a re-definition of the internal logic. Large organizations (such as DoD) may be less adept at coping with change." [3] C&A under the DITSCAP is an embedded process, and a revision of this process will require significant new learning across DoD.

Net-Centric C&A

Despite the challenges anticipated by the inevitable change to the current DITSCAP C&A process, DoD must address a net-centric approach to C&A. The vision of a net-centric C&A can be best described as networked C&A activities accomplished through distributed collaboration processes designed to ensure that all pertinent available system-security information is dynamically managed, visible, and shared.

The DIACAP

The DIACAP is DoDs approach to implementing a C&A process that supports net-centricity. Its approach is based on the following:

- Standard, ubiquitous IA services founded on community best practices
- A common data dictionary and uniform, data-centric, highly reusable system documentation
- Early and continuous collaboration facilitated by electronic information-exchange standards
- Dynamic, asynchronous, and multi-agented verification and validation
- Capabilities- and performance-based accreditation and re-accreditation decisions
- Integration of IA process and reporting requirements; (*e.g.*, the Joint Quarterly Readiness Review (JQRR), the Federal Information Security Management Act (FISMA), and the Information Assurance & Vulnerability Assessment (IAVA)].

Currently in draft status and slated to supersede the DITSCAP in the coming months, the DIACAP establishes the DoD process for C&A based on the concepts of IA that are expressed in the form of IA Controls.

IA Controls

In the context of the DIACAP Instruction, an IA control is "an objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format." In other words, an IA control is a standardized, formatted expression of a specific IA requirement. The IA Controls are aligned along two continuums, MACs and Confidentiality Levels, and serve as the primary tools for identifying, implementing, and validating IA measures for DoD information systems. (See Figure 2.)

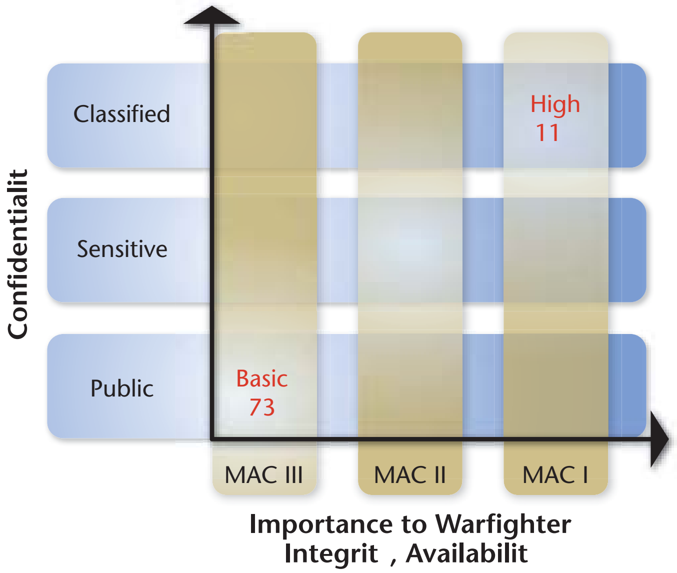


Figure 2. Assignment of IA Controls in Alignment with MACs and Confidentiality Levels

The DoDI specifies that DoD information systems will implement the IA Controls based on determinations regarding (1) the system's Confidentiality Level and (2) the system's MAC. IA Controls are grouped into the following subject areas:

- Security design and configuration
- Identification and authentication
- Enclave and computing environment
- Enclave boundary defense
- Physical and environmental, personnel, continuity
- Vulnerability and incident management

Providing Solutions for a Net-Centric C&A Program

People and Process Solution: the DIACAP

Defense in Depth (DiD) emphasizes a multi-faceted approach based on people, process, and technology. The DIACAP leverages the community and consensus-based best practices incorporated into IA Controls (DoDI 8500.2), into a C&A process that is less document intensive. The goal of DIACAP is to identify and verify IA Controls for systems, to establish a standard approach for documenting and sharing the IA posture of systems, and to standardize the authorization process for these systems in a decision and governance structure that spans the entire enterprise. DIACAP also provides a method for managing the IA posture across DoD information systems that is consistent with FISMA guidelines.

DIACAP will also initiate a more dynamic review and validation program than that established under DITSCAP. At least annually, DIACAP requires a review of selected activities and IA Controls. In other words, DIACAP requires continual assessment of IA Controls and the exposure of the IA Controls status to date to the net. DIACAP is aligned into activities, rather than into the strict, monolithic phases of the DITSCAP. (see Figure 3)

Rather than a single, monolithic SSAA, C&A documentation under DIACAP will be organized into a collection of artifacts that can be assembled into various combinations, as required. DIACAP documentation requirements will be limited to information generated by the C&A process or information required to make a C&A decision; these requirements should not repeat information available in other sources. For example, system description and architecture information is clearly required for information system security engineering; however, it exists outside of C&A and, therefore, can be captured as a C&A artifact that does not require re-creation for the SSAA. A security or IA architecture that shows the logical placement and relationships of IA solutions is also an IA artifact and should be included as one under the appropriate IA Control (DCFA–Functional IA Architecture for Automatic Identification System (AIS) Applications).

Technical Solutions: eMASS, the DIACAP Knowledge Service and VAMS

eMASS

eMASS is a joint research initiative of the Office of the Assistant Secretary of Defense, Networks & Information Integration [OASD(NII)]; the Defense Logistics Agency (DLA); and DoD Information Assurance Technology Analysis Center (IATAC). eMASS is the centerpiece of an ongoing DoD effort to develop and implement an array of technical initiatives that re-engineer and automate a broad range of IA functions to deliver a comprehensive, fully integrated IA management capability at the enterprise level for DoD Components CIOs. The system is specifically designed to support the people and process requirements of DIACAP.

The primary vehicles for accomplishing this objective include standardizing DoD IA processes and developing a common IA architecture framework and low-cost, flexible, universally accessible automation using relational databases and Web-server technology. eMASS seeks to provide this through an integrated suite of government-owned, relational-database management systems, based on Commercial-off-the-Shelf (COTS) components and accessed through an associated Web interface, which will improve IA program management by standardizing approaches for describing and collecting required data for C&A and other core IA functions.

The C&A Module provides a Public Key Enabled (PKE) role and organization access-control scheme that implements workflow at both the C&A package and the

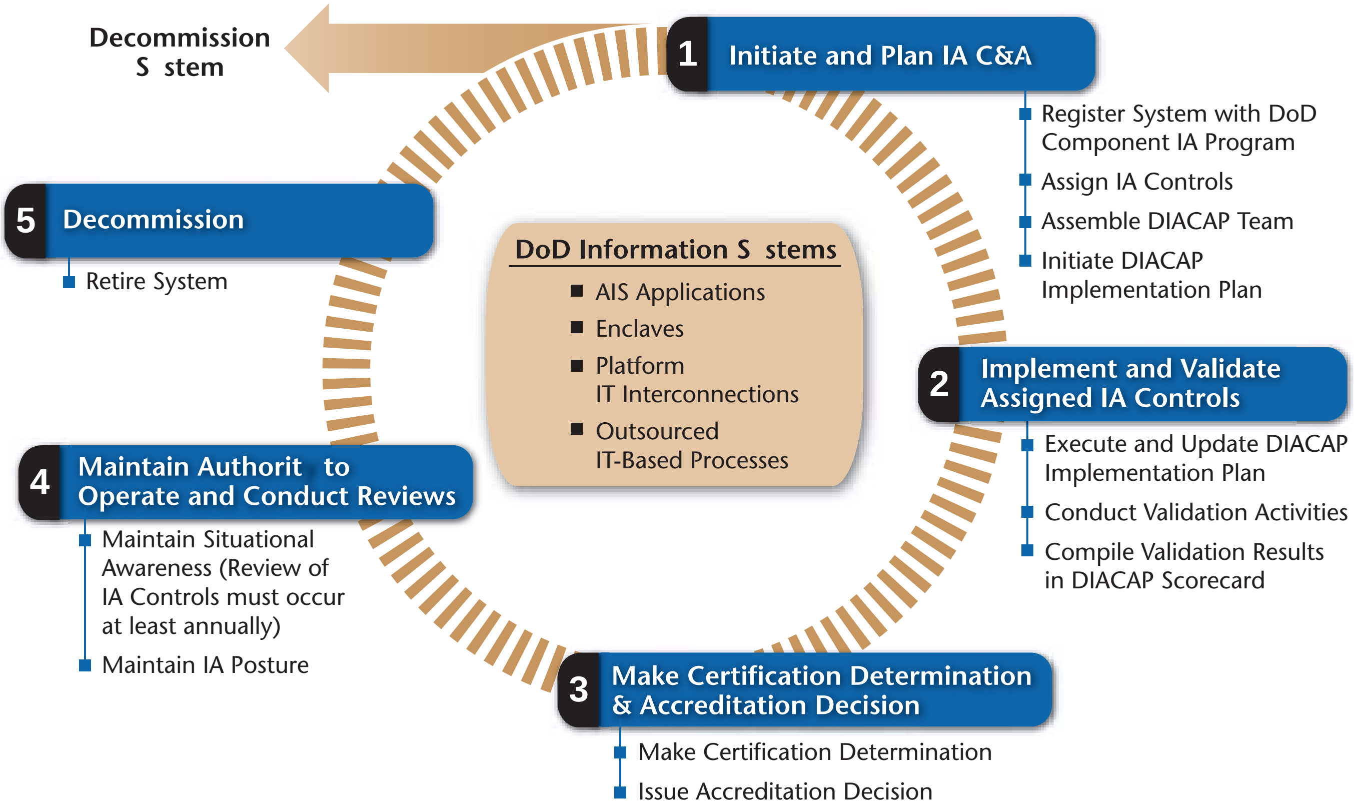

Decommission
S stem
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
2 Implement and Validate Assigned IA Controls
Execute and Update DIACAP Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authorit to Operate and Conduct Reviews
Maintain Situational Awareness (Review of IA Controls must occur at least annually)
Maintain IA Posture
5 Decommission
Retire System
DoD Information S stems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes

Figure 3. DIACAP Activities

individual IA Control levels. As C&A actions are worked, they are electronically "moved" through the in-boxes of the assigned DIACAP team. Completed actions are digitally signed. The owning "enterprise" or IA Program has the flexibility to establish roles and workflow rules. All information in the system is available for query and standard reports, subject to access controls. The owning "enterprise" also has the ability to develop its own reports. The registration module includes a number of customizable fields that enable the owning enterprise to flag and filter information according to its business processes and management needs.

eMASS is designed to correlate data to meet FISMA requirements and automatically produce all FISMA reports, including Plans of Actions & Milestones (POA&Ms) and self- assessments. The eMASS registration process within the C&A Module implements organizational hierarchies and system boundaries and interconnections through an extensible parent-child model. For the purposes of accessing data, reporting, and assigning IA Controls, both organizations and systems may have multiple parents. Systems may be wholly nested or may share or inherit IT components or IA Controls.

The DIACAP introduces, the concept of an electronic rating system used to gauge the collective compliance status of IA Controls within a DoD information system deployed in the GIG. This status will form the basis for the net-centric exchange of system-security credentials. eMASS is expected to be integrated with the IA Core Enterprise Services (CES) to serve as the communications mediator for these system-security assertions between DoD systems connected to the GIG infrastructure. This mediation will be based on the exchange of security credentials, which are based on a "scorecard" developed by using eMASS to manage the C&A process and validate the systems-security status. By visualizing the IA Control compliance status and the corresponding system-security status, the DIACAP Scorecard (a.k.a. the Digital Scorecard), tabulates the results of the control association and validation processes.

The eMASS application suite was developed using the Net-Centric Enterprise Services (NCES) System Development Kit (SDK), which operates with either Oracle or Microsoft Structured Query Language (SQL), is completely enabled for Web services and eXtensible Markup Language (XML), and is designed to be completely extensible in its deployment. Deployment can be either logical or physical. Multiple logical instances can be physically collocated (*e.g.*, in a Defense or a DoD Component data center) or physically distributed (*e.g.*, on board a ship or throughout DoD Component Enclaves). Transient eMASS nodes—those aboard ships or in tactical environments—can be automatically synchronized with their deployment tree on re-entry into the net. Figure 4 illustrates deployment flexibility.

The first operational pilot for the eMASS application suite was deployed in early FY 04 with an embedded Knowledge Base containing the IA Control implementation and validation guidance. During FY 05, the re-designed net-centric eMASS and an external Web-portal Knowledge Service will be deployed in multiple additional pilots throughout DoD.

Future eMASS spirals may include logic that digests itemized scorecard information into a set of numerical expressions—an IA "score." The score value will ostensibly denote the current level of system compliance within a predetermined range—from non-compliance to full compliance—on a dynamic scale. The manner in which this score will be used is still being defined within the eMASS program; however, it is expected that the score may serve as a form of IA "token" that will be exchanged without human interface and analyzed at the system level as a pre-

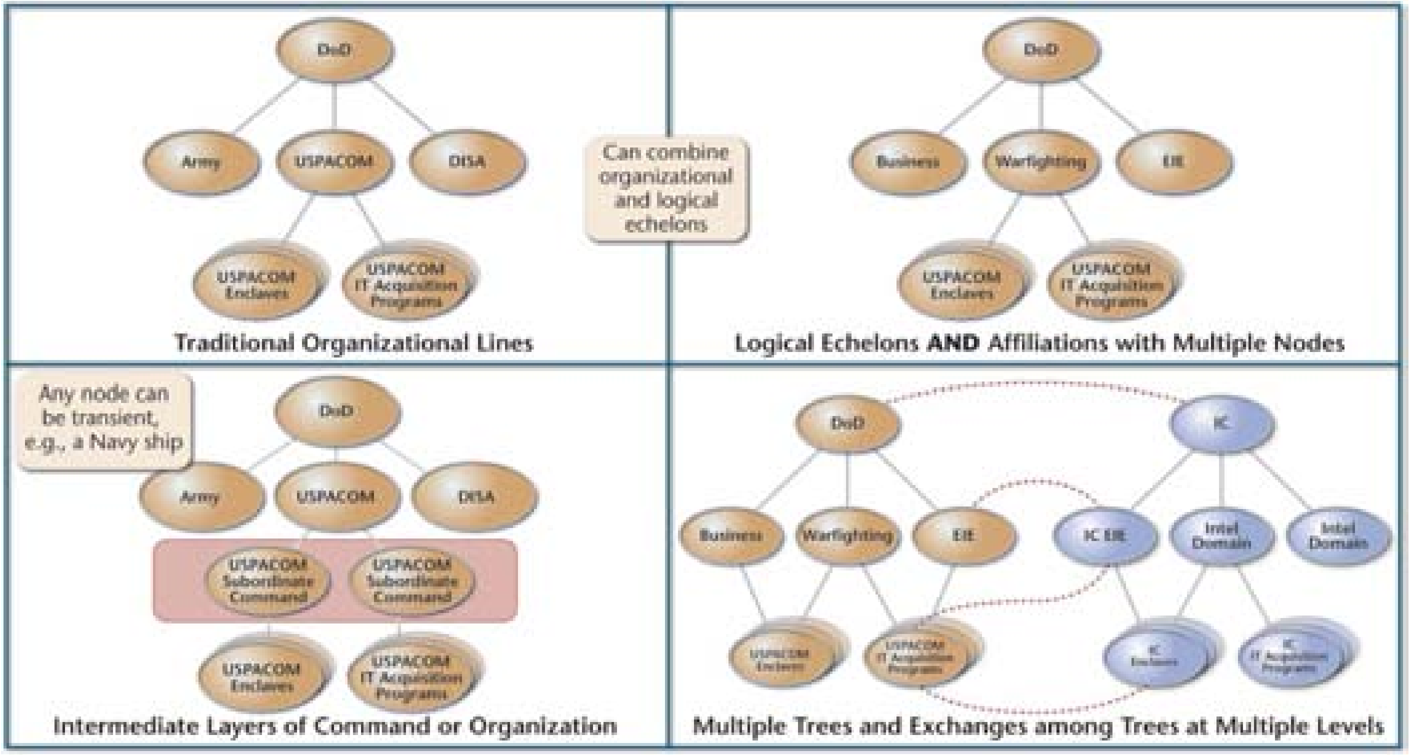

DoD
Army
USPACOM
DISA
USPACOM Enclaves
USPACOM IT Acquisition Programs
Traditional Organizational Lines
Can combine organizational and logical echelons
DoD
Business
Warfighting
EIE
USPACOM Enclaves
USPACOM IT Acquisition Programs
Logical Echelons AND Affiliations with Multiple Nodes
Any node can be transient, e.g., a Navy ship
DoD
Army
USPACOM
DISA
USPACOM Subordinate Command
USPACOM Subordinate Command
USPACOM Enclaves
USPACOM IT Acquisition Programs
Intermediate Layers of Command or Organization
DoD
IC
Business
Warfighting
EIE
IC EIE
Intel Domain
Intel Domain
USPACOM Enclaves
USPACOM IT Acquisition Programs
IC Enclaves
IC IT Acquisition Programs
Multiple Trees and Exchanges among Trees at Multiple Levels

Figure 4. eMASS Deployment Options

requisite for initiating a communication session between two GIG hosts. Presuming a simple line of communication between two hosts, eMASS will mediate the session request and compare the two IA scorecard values. Based on the values directly or in conjunction with some set of predetermined security conditions, eMASS may permit or deny the session and consequently permit a host-to-host connection or force a communication termination. This process is illustrated in Figure 5.

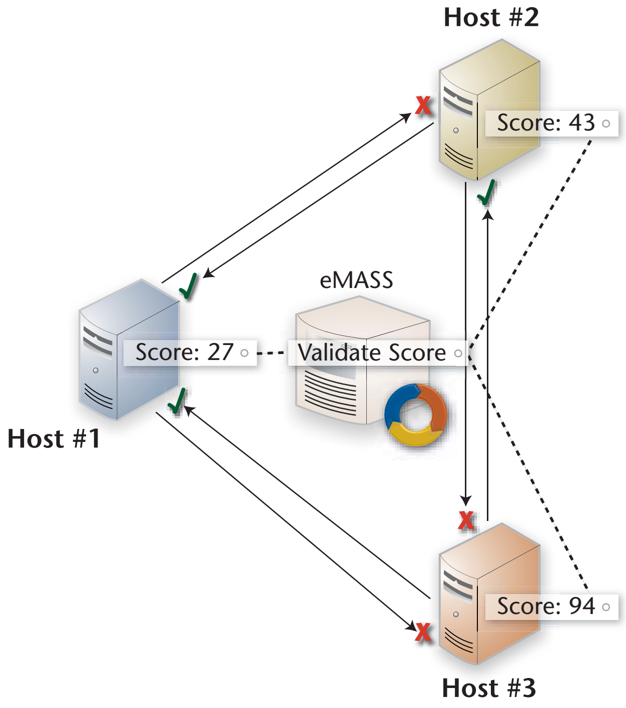


Figure 5. Notional Host-to-host Connection Process

The DIACAP Knowledge Service

The heart of eMASS functionality is the DIACAP Knowledge Service, an online repository of IA Controls sets authorized by the GIG. Initially, the Service will include DoDI 8500.2, and later expansion will include the Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems, and any special sets or augmentations developed by DoD Components, GIG Mission Areas, Domains, or Communities of Interest (COIs). In addition to the IA Controls themselves, the Knowledge Service includes rules for assignment, annual or other review, reporting, implementers, and standardized validation procedures, including community-vetted expected results. The community-vetted expected results ensure reciprocity among certifiers and accreditors. The validation procedures may include links to or information about automated testing tools. Examples of implementers include, but are not limited to, Architecture Guides; Design Guides; Enterprise Information Environment (EIE) Interface Specifications; Acquisition or Contract Aids; IA/IT Product Configuration Guides; Statements of Practice; NetOps Security Administration Tactics, Techniques, and Procedures (TTPs); and Network Defense Guidelines. Figure 6 provides the architectural representation of the Knowledge Service content to support DoD IA Controls environment.

In addition to the specific information related to IA Controls, the Knowledge Service contains the following:

- Comprehensive instructions of recommended mechanisms to facilitate the transition from DITSCAP to DIACAP
- A library of tools, diagrams, process maps, *etc.* to support and aid in executing the DIACAP

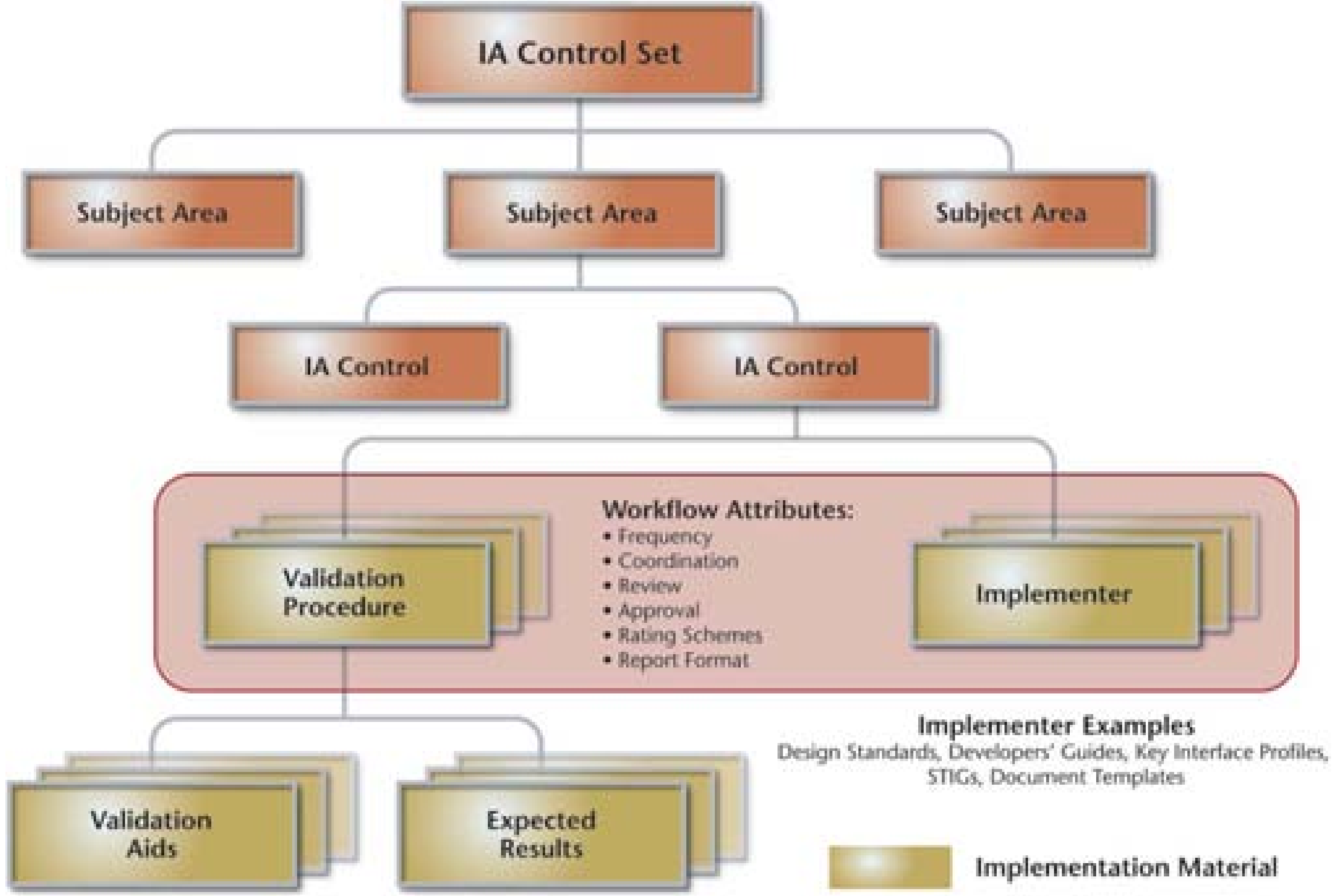


Figure 6. Representation of an IA Control Set Schema in the DIACAP Knowledge Service

- A collaboration workspace for the DIACAP user community to develop, share, and post lessons learned and best practices
- A source for IA news and events and other information related to IA information resources, including links to training

The DIACAP Knowledge Service is intended to be available in all GIG security domains, to be deployed concurrent with new DIACAP Instruction, and to have three access paths, as depicted in Figure 7:

- Direct user access and collaborative capability through a Content Management Portal
- A back-end authoring, staging, approving, and Configuration Control Management (CCM) and Knowledge Management capability for authorized members of DIACAP's Technical Advisory Group, its Configuration Control Board, and the IA staff of OASD(NII)
- Full Integration in the eMASS application suite and access through the eMASS C&A Module
  - In this scenario, a user interacts with eMASS to implement DIACAP, as described in DIACAP Instruction. DoD information systems are registered in the DIACAP Registry, which interfaces with DoD IT Registry and other IT applications, as required. System characteristics identified during registration establish the system's baseline IA Control set. The DIACAP team then has the opportunity to interact with the Knowledge Service to expand or modify the assigned IA Control set within the policy parameters established by the governing DoD Component IA Program.

VAMS

The VAMS system and its supporting conceptual framework are generating a growing degree of interest among its represented customers and many other groups affiliated with developing the GIG. VAMS is intended for near-term integration with eMASS to provide additional functionality. Engineered by professionals knowledgeable in both IA concepts and emerging technologies, the VAMS system has been designed in a parallel effort to that of the eMASS. This effort will leverage the service-oriented aspects of the GIG, using state-of-the-art tools and technologies, while maintaining a strong adherence to commercial and government IA best practices.

In essence, VAMS is a data-consolidation utility, designed to gather from various sources the IA information specific to a system or group of systems and to correspondingly re-package this information into a common, consolidated representation of IA posture. The VAMS system is not intended to be used as a replacement for existing IA assessment products; rather, it should be used as a supplementary collaboration utility for organizing and analyzing data, in a more centralized manner, collected by distributed components.

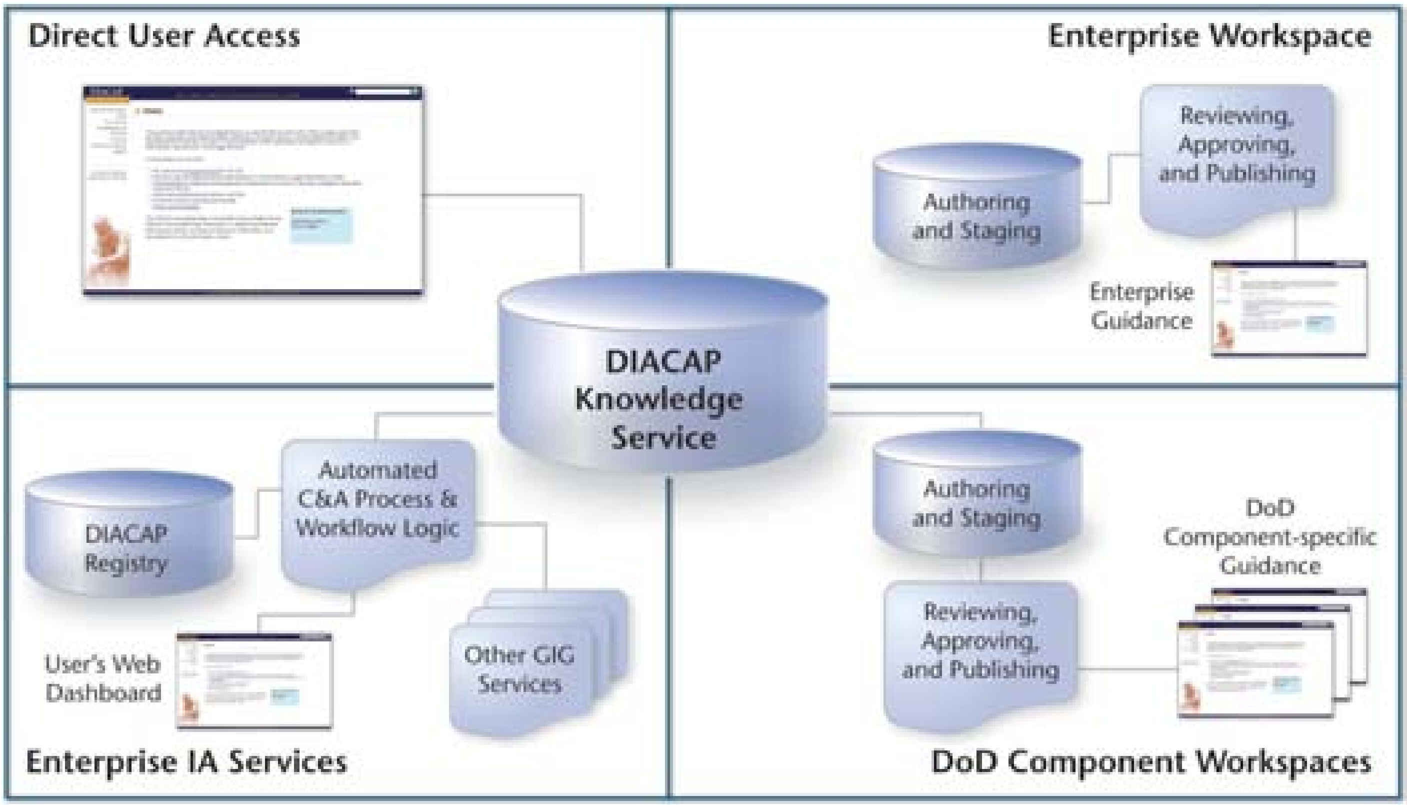


Figure 7. eMASS and Knowledge Service Access Paths

Assuming a reconciliation of hosts deployed throughout the GIG, eMASS and the associated core processes also require data that is relevant to the security postures of these hosts, including vulnerability status and configuration parameters. This data may be supplied through a variety of sources, as indicated in Figure 8.

Though not illustrated in the diagram, the VAMS framework is being designed to execute much of the necessary back-end processing to supply eMASS with the required data to perform IA Control associations. VAMS will accomplish this by performing the following general activities in response to a data request through the eMASS interface:

- Polling the back-end COTS tool for a list of vulnerabilities native to an identified host or group of hosts
- Formatting the returned data into a common, extensible representation through XML
- Propagating the formatted data through an intermediate Web service that aggregates returned data from additional sources
- Propagating the formatted data aggregate up to eMASS for storage in a local database for future processing or for viewing directly through the eMASS user interface

From an IA standpoint, Vulnerability Management (VM) may be considered to encompass a broad spectrum of security disciplines. While relevant to a comprehensive Risk Management portfolio, many security disciplines are currently out of the scope of the VAMS program and framework. Within the context of VAMS, the concept of "Vulnerability Management" has been generalized to include only information that is related to IA and is currently accessible through the use of commonly implemented, commercially available Vulnerability Assessment tools, such as the following:

- ISS RealSecure
- Harris STAT (Security Threat Avoidance Technology) Scanner
- Eeye Retina
- Nessus Scanner
- Others, such as Virtual Memory System (VMS)

Rather than returning the full contents of a VM tool database, VAMS extracts only those elements necessary to construct accurate IA composites of assessed hosts that use these tools. The following is an abridged list of some of the elements that may be relevant to creating such composites:

- Vulnerability ID (vendor assigned)
- Vulnerability name (vendor assigned)
- Vulnerability description
- Affected host identifier, such as network name, Internet Protocol (IP) address, and/or MAC address

The VAMS uses the terminology "Asset Management" in the context of identifying Assets or items connected to networks. It does not currently address the typical "Asset Management" functionality as the term is used in accounting, inventory, and purchasing. Asset Management, or in this case, Asset Identification, is key to identifying assets; *i.e.*, the items that are residing on the network.

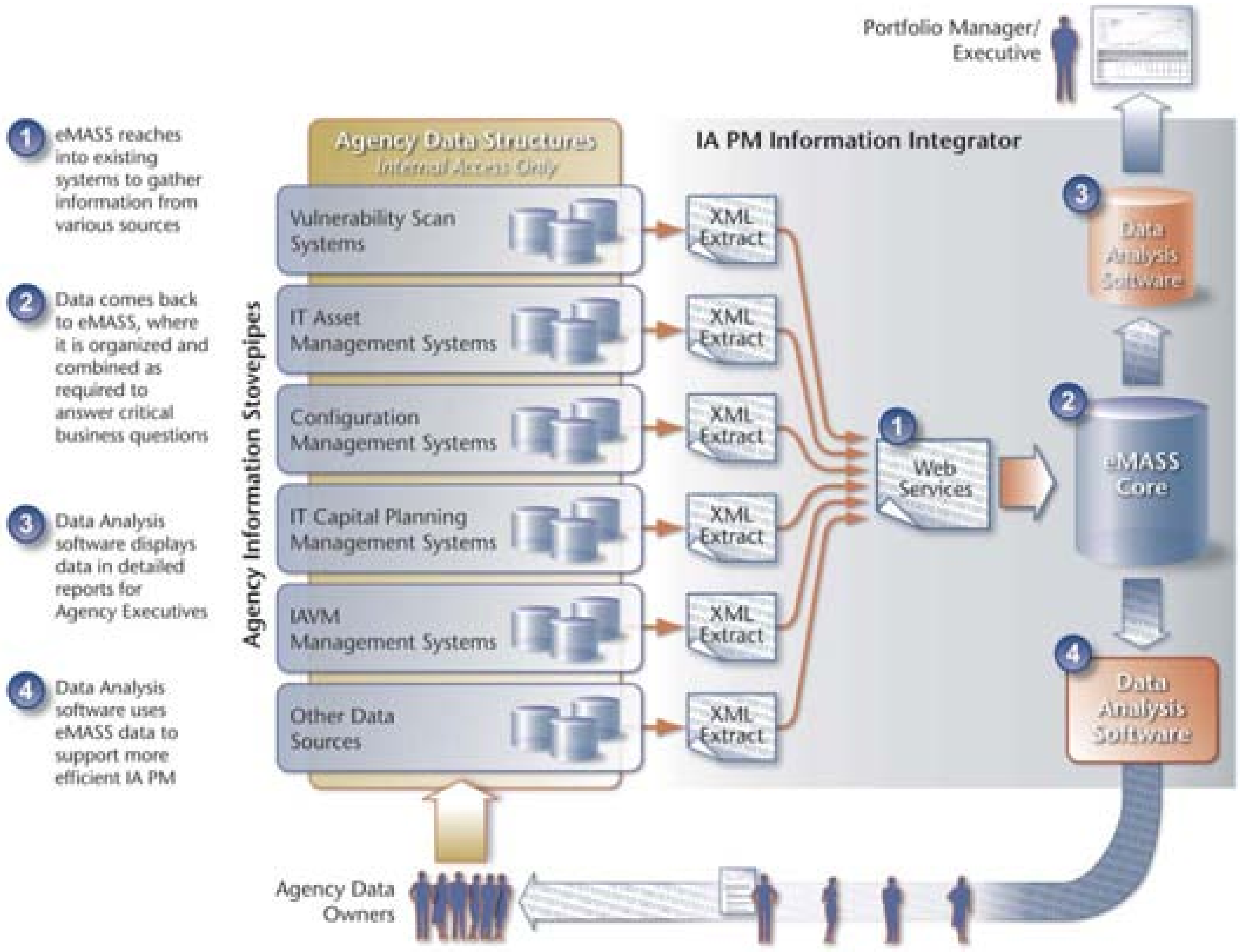

Portfolio Manager/ Executive
1 eMASS reaches into existing systems to gather information from various sources
2 Data comes back to eMASS, where it is organized and combined as required to answer critical business questions
3 Data Analysis software displays data in detailed reports for Agency Executives
4 Data Analysis software uses eMASS data to support more efficient IA PM
Agency Data Structures
Internal Access Only
Agency Information Stovepipes
Vulnerability Scan Systems
IT Asset Management Systems
Configuration Management Systems
IT Capital Planning Management Systems
IAVM Management Systems
Other Data Sources
IA PM Information Integrator
XML Extract
XML Extract
XML Extract
XML Extract
XML Extract
XML Extract
1 Web Services
2 eMASS Core
3 Data Analysis Software
4 Data Analysis Software
Agency Data Owners

Figure 8. eMASS Data Input Sources

The term "Configuration Management" is used by this program in the context of discovering specific asset-data attributes; *i.e.*, detailed information of the identified network-asset items. The use of configuration data is critical to collecting information for analyzing potential vulnerabilities.

VAMS collects data on asset-configuration attributes to discover potential vulnerabilities. Vulnerabilities are typically identified within network assets through configuration-attribute data. To do this, VAMS polls each asset item connected to the network and system to gather defined information. The information is then correlated within eMASS and VAMS. A comparison of the vulnerability policy and the asset-configuration attribute data is completed, and a report is generated that identifies assets and specific attributes with potential vulnerabilities.

Managing a Net-Centric C&A Process Through an Integrated Program

IA is a discipline characterized by many processes that are often conducted in an independent or stovepiped fashion. Each process establishes its own information needs and reporting requirements. At an individual system level, information must be collected and managed differently for each process, which is expensive and counterproductive. At DoD Component or command level, correlation and comparison is difficult because naming conventions, definitions, and reporting frequency vary by IA process.

DIACAP establishes a consistent process based on IA Controls as a standard unit of reporting. This process is intended to reduce the data collection and reporting burden at the individual system level and concurrently improves systems-security data correlation and analysis at DoD Component or command level. The DIACAP Knowledge Service supports DIACAP by providing a supporting set of guidance required for consistent implementation, validation, and certification of system-security processes based on IA Controls. eMASS provides the automated capability intended to facilitate the execution of C&A under DIACAP and a flexible architecture that permits modular expansion to support multiple facets of IA program management. Finally, when integrating into eMASS, VAMS will make available the data required to further align C&A status with Vulnerability, Asset, and Configuration Management.

The entire suite of capabilities provides a strong foundation for dynamic system-security management and visibility of IA posture across the GIG.

Recent research has focused on using an assertion model for the exchange of security-related credentials. The greatest applicability explored thus far has been the exchange of user credentials for electronic business or for authenticating to the network. Through this integrated program, an assertion model such as this one could be extended to information systems. An accredited information system could be assigned an electronic credential containing its IA posture, its accrediting authority, *etc.* This credential could be "asserted" on demand as part of a connection negotiation. Advantages of such an approach would be significant if the model were only internal to DoD, particularly for military systems that must rapidly deploy and "connect on demand." As the calculation of an IA posture becomes more automated and thereby more current, such credentials could also store and assert a readiness rating. Eventually, this same model could be extended to facilitate connections with other government agencies, trading partners, and coalition partners.

Benefits of this Approach

A Net-Centric approach to C&A has many benefits:

- The time and expense of each system individually identifying IA requirements to counter general IT threats and vulnerabilities, satisfy DoD policies, and conform to operational or technical requirements across the GIG is mitigated.

- DoD has established the baseline set of IA Controls; however, DoDI 8500.2 permits supplementation at DoD Component and the information systems levels in an organized and systematic manner. This hierarchy of IA Control development and issuance permits IA Controls to be developed once for the broadest audience but supplemented for individual organizational requirements. This provides a channel for effective use of IA resources, broadened application of technical expertise, and standardization of IA requirements and solutions.

- IA Controls and supporting information can be maintained and promulgated through the DIACAP Knowledge Service. Using a Web-portal environment for the IA Controls support structure permits rapid evaluation and modification of IA Controls, as required by the demands of emerging environments.

- Implementation guidelines for IA Controls can be organized, packaged, and managed for each IA Control within the DIACAP Knowledge Service. This permits DoD to establish baseline-implementation guidelines that apply to the entire GIG, thereby promoting standard, interoperable IA services and permitting DoD Components and systems to supplement the guidelines, as appropriate.

- C&A packages need not include the implementation guidelines and testing procedures that are available online; thus the package should be smaller, easier to produce, easier to read, and easier to automate.

- Responsibility for meeting the IA Controls can be shared between DoD information systems (*e.g.,* an AIS application and its hosting enclave(s) or a platform IT interconnection and connecting enclave). Systematic allocation of responsibilities enables and promotes accountability, collaboration, and shared solutions.

- Designated Approval Authorities (DAAs), CIOs, Commanders, and other decision authorities can have a definition of adequate security accepted by the community and a framework for (1) assessing an individual system's IA capabilities and (2) a framework for comparing multiple systems.

- Compliance standards and readiness metrics can be associated with IA Controls. The Security Testing & Evaluation (ST&E) activities within C&A can return readiness and compliance indicators.

- Compliance standards and readiness metrics associated with IA Controls would provide a means to quickly and easily discuss or exchange the IA posture of information systems, which should facilitate connection decisions by replacing the current practice of requiring another round of ST&E and a reformatting of system documentation.

- Validation-testing processes for each IA Control can be organized, managed, and updated in association with the IA Control itself. This further helps to standardize both the IA solution and the requirement and to standardize the information available about conformance to the requirement.

- The list of IA Controls assigned to a DoD information system can be modified without re-starting the entire C&A process. An IA Control can be assigned, modified, or retired at any time, and only the "clock" for conformance to that particular IA Control is impacted.

- IA Controls can be assigned an appropriate testing or validation frequency. Not all IA Controls need to be tested together on an annual cycle. This permits testing or certification to align to the rate of change.

- Customizing the C&A process for currently identified types of DoD information systems helps focus on differing critical IA quality indicators and promotes accountability. Understanding the process for these information systems facilitates developing tailored processes for other, emerging information-systems environments.

- Managing C&A packages in accordance with DIACAP and through the use of the DIACAP Knowledge Service and eMASS permits the process to scale to evolutionary acquisition and large complex systems, families of systems, and systems of systems.

Next Steps

The DIACAP instruction is nearing approval and publication. Upon publication, DoD Components will be provided access to the DIACAP Knowledge Service. eMASS pilots will continue, along with VAMS integration.Work also continues on the selection and definition of additional modules for eMASS. These include modules for IA metrics, privacy implementation and Privacy Impact Assessments (PIAs), IA training and certification tracking, and others.

Finally, working groups are considering the design of additional IA Control Sets to implement within eMASS and the Knowledge Service. Among these are IA Controls based on the National Institute of Standards (NIST) 800 37/53; the DCID 6/3 requirements for the Intelligence Community; the requirements of Cross Domain Security and Coalition environments; and others. ■

References

Alberts, David S. and Hayes, Richard E. "Power to the Edge: Command, Control in the Information Age." CCRP Publication Series, June 2003.

Department of Defense Brochure, "Mission: Possible–Security to the Edge," 2005.

DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002.

Office of Management & Budget (OMB) Circular A-130, Management of Federal

Information Resources, defines adequate security as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

Moffat, James. "Complexity Theory and Network Centric Warfare." CCRP Publication Series, September 2003.

Pullen, William. "Strategic Shocks: Managing Discontinuous Change." International Journal of Public Sector Management, Vol. 6, No. 1, 1993, pp. 30-39.

Turner, Glenda. "DoD Information Assurance Certification and Accreditation Process—The Next Generation (DRAFT)," February 2003.

About the Authors

Glenda Turner

Ms. Glenda Turner is a Senior Policy Advisor in the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Networks and Information Integration [OASD(NII)]. Her current focus includes the information assurance (IA) component of enterprise architecture, establishment of an enterprise IA portfolio and management process, and enterprise IA governance. She is a computer scientist and former military officer, and she was worked throughout the Department of Defense in communications, information, intelligence, and infrastructure.

Julie E. Mehan

Dr. Julie Mehan manages several projects for Department of Defense (DoD). She has over 25 years of experience in various DoD and Intelligence agencies. Dr. Mehan's previous experience includes US Government Service, most recently in developing, designing, and leading the Department of the Army's Information Operations Vulnerability Assessment and Red team Division (IOVAD). In this capacity, she participated in multiple International, Joint, and Army deployments, providing both real-world and exercise support. Dr. Mehan graduated Summa Cum Laude with a PhD in Organization and Management from Capella University, Minneapolis, Minnesota. This program focused on research into the issues and challenges facing Chief Security Officers (CSOs) in large government and commercial organizations and resulted in the development of a dynamic model of CSO leadership. She holds an MA degree with Honors in International Relations and Law from Boston University and a BS degree in History and Languages from the University of New York.

Michael Colon

Mr. Michael Colon has managed various projects for the Defense Information Systems Agency (DISA). He was Technical Lead in support of the Ports and Protocols Registration Database System; headed the Java development effort throughout the life cycle of the project; and implemented DISA's Secure Technical Implementation Guidelines for UNIX, NT, Oracle, and iPlanet on all production servers, which were tested and approved by the DISA Field Security Officers (FSO) review. He also worked with team members to develop the SSAA for the system to ensure that the system would be approved and accredited for use on the NIPRNET. Mr. Colon holds a BS degree in Computer Science with a mathematics minor from Hofstra University, Uniondale, New York, and is a Sun Certified Java programmer for the Java 2 platform.

Patrick Holley

Mr. Patrick Holley, CISSP, has 6 years of experience in IA/IT and has served as the primary author for products developed in support of the Vulnerability Assessment Management Service (VAMS) System. His background includes experience in government IA/CND architecture design, engineering, analysis; DoD IA Policy; and secure software architecture, requirements analysis, and design. He has authored/co-authored numerous whitepapers promoting software assurance and emerging technology R&D within the DoD and GIG communities, and he is currently contributing to a draft NIST Special Publication for secure web services.

IATAC Spotlight on Research

Dr. Rusty Baldwin

by Ronald Ritchey

This article is the third in a series of profiles of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. Information Assurance (IA) and Information Operations (IO) experts from many different organizations volunteer to be IATAC SMEs and provide information on their areas of expertise, education and training, professional certifications, inventions, and patents. When the US Department of Defense (DoD) or other government personnel contact IATAC with questions regarding IA or IO, IATAC can leverage its SME database to identify people who are particularly well suited to answering those questions. SMEs are also encouraged to contribute papers and other materials to IATAC's Scientific and Technical Information (STI) collection. The work of the SMEs furthers our understanding and capabilities in IA.

The IATAC SME profiled in this article is Dr. Rusty Baldwin, an associate professor with the Center for Information Security Education and Research (CISER) [1] at the Air Force Institute of Technology (AFIT), Wright Patterson Air Force Base, OH. [2] His primary areas of research include wireless traffic analysis and exploitation, wireless ad hoc networks, digital design, and wireless protocols for sensor networks. Dr. Baldwin received his PhD degree in Electrical Engineering from Virginia Polytechnic Institute and State University in 1999. He is a co author of the recent conference paper, *Developing an Insider Threat Model Using Functional Decomposition*, and has published papers in several other IA related journals.

Dr. Baldwin conducts research in energy efficient wireless sensor networks, reconfigurable computing, and geolocation of Internet Protocol (IP) address nodes based on latency. Dr. Baldwin is also involved in the Department of Homeland Security (DHS) Software Assurance Program, an initiative to develop a common body of knowledge for software assurance. This initiative is intended to document the knowledge required to produce secure software. It is unique in that it approaches the issue from three angles—acquisition, development, and sustainment. The acquisition phase addresses the problem of assuring software that is obtained from external vendors or sources, and the activities in this phase run the gamut from certifying vendors to writing secure wrappers for the software. The development component addresses how to mitigate security risks during code development by using best coding practices, tools, and testing techniques. Finally, the sustainment aspect of the DHS program addresses the ubiquitous problem of maintaining an acceptable level of security assurance of deployed software, even in the face of ever evolving threats from sophisticated attackers and new strains of viruses, worms, and other malware.

Dr. Baldwin has recently leveraged his wireless network expertise to develop an AFIT originated approach to covert monitoring of Bluetooth networks. Every 625 nsec, a Bluetooth radio switches its transmission frequency. This is commonly referred to as hopping to a different channel and is based on a pattern called the hop sequence. While communicating with one another, Bluetooth devices must use the same hop sequence to successfully complete a session. The method Dr. Baldwin and his recently graduated PhD student, Dr. Brian Peterson, have developed monitors the energy levels in a given Bluetooth Personal Area Network (PAN). Using this information, the hop sequence can be deduced, thereby permitting devices to synchronize with a Bluetooth device without explicitly requesting to do so. This classified research was been published in 2003 and 2004 in the proceedings of the Military Communications Conference (MILCOM) and was awarded the Lt Gen Gordon T. Gould Award for best classified paper.

If you have a technical question for Dr. Baldwin or other IATAC SMEs, please contact iatac@dtic.mil. The IATAC staff will assist you in reaching the SME best suited to helping you solve the challenge at hand. If you have any questions about the SME program or are interested in joining the SME database and providing technical support to others in your domains of expertise, please contact iatac@dtic.mil, and the URL for the SME application will be sent to you. ■

References

[1] http://en.afit.edu/ciser/
[2] http://www.afit.edu

DoD Information Assurance/ Computer Network Defense (IA/CND) Enterprise-wide Solutions Steering Group or ESSG

by Wayne Wise

This is the first in a series of articles about the Information Assurance/Computer Network Defense (IA/CND) Enterprise-wide Solutions Steering Group (ESSG) of the US Department of Defense (DoD). Because of the rapid pace of ESSG's solution acquisitions and implementation, these articles provide a timely method of informing the IA/CND community of both the group's activities and details of emerging solutions.

The ESSG is a unique example of joint cooperation supporting rapid acquisition. The ESSG was chartered in 2003 to integrate and synchronize solutions, to advocate adherence to IA strategic goals, and to field enterprise-wide CND solutions. Commander, United States Strategic Command (USSTRATCOM) uses the ESSG as one means by which to fulfill the Unified Command Plan's responsibility for defending the Global Information Grid (GIG). ESSG activities are focused on fast acquisitions of near-term, enterprise-wide solutions that support current operational requirements.

Chaired by USSTRATCOM, the ESSG has voting members from all four services; the US Joint Forces Command (JFCOM); the Joint Staff Command Control, Communications, and Computer Systems Directorate (J6), which represents all non-voting combatant commands; the Defense Information Systems Agency (DISA); the Defense-wide Information Assurance Program (DIAP) of the Assistant Secretary of Defense (Networks & Information Integration) (ASD[NII]); the Defense Intelligence Agency (DIA); and the National Security Agency (NSA).

To deliver quality products to the field, the ESSG established a Technical Advisory Group (TAG), an Acquisition Working Group (AWG), a CND Architecture Working Group (CAWG), a Project Management Office at DISA, and a Concept of Operations (CONOPS) Working Group at JFCOM. These groups provide the Subject Matter Experts (SMEs) to help establish technical requirements, develop systems architectures, write contractual documents, and publish CONOPS. Solutions are certified and accredited by DISA's Field Service Office (FSO), which is charged with joint-service implementation. Each service is responsible for accrediting and implementing products within their respective services.

The ESSG team has already delivered DoD enterprise-wide licenses for the following:

- **e-EYE Retina**—Secure Configuration Compliance Validation Initiative (SCCVI), a network- and vulnerability-scanning tool, used to check compliance with Information Assurance Vulnerability Alert (IAVA).

- **Citadel Hercules Secure Configuration Remediation Initiative (SCRI)**—A tool used to patch the vulnerabilities found by SCCVI. Having completed their pilot deployments, SCCVI and SCRI have moved into their deployment phase across DoD.

- **e-Trust PestPatrol**—Spyware Detection and Eradication Program (SDEP), an Adware/Spyware program, used to protect DoD computers from attacks such as key-loggers and screen scrapers. SDEP is available now for home use while it completes the 120-day pilot deployments.

What lies ahead for the ESSG? In FY 2006, the ESSG will procure a Host-Based Security System (HBSS), a Tier 3 (Base/Unit-Level) Security Information Manager (SIM) tool, and a tool to help mitigate insider threats. The ESSG team is also working on hardening the Secret Internet Protocol Router Network (SIPRNet), mitigating the wireless threat, and procuring components of an Enterprise Sensor Grid (ESG) and User Defined Operational Picture (UDOP). Future articles will discuss these procurements and initiatives in further detail. ■

eEye Digital Security
Vulnerability Management Solutions
Retina® Network Security Scanner

Figure 1: http://www.eeye.com

Figure 2: http://www.citadel.com

Figure 3: http://www.pestpatrol.com

About the Authors

Wayne Wise

Mr. Wayne Wise has 29 years in IA, network engineering, satellite communications, and telecommunications security. As a Global Information Assurance Specialist, he supports the Commander, US Strategic Command in his Information Operations mission. Mr. Wise works as a subject matter expert for the ESSG, and supports IA issues for the many Joint Capability Integration and Development System (JCIDS) documents in which USSTRATCOM is involved. While at Air Force Material Command, Mr. Wise was Chief of Operations for the Network Operations and Security Center (NOSC), as well as ISSO and ISSM for the special projects branch. He designed and installed the USAFE Secure Data Access (RASP) program. He holds CIO and NSTISSI No. 4011 certificates from NDU, as well as certifications from Microsoft and Comptia.

IATAC Spotlight on Research and Education

Air Force Institute of Technology (AFIT)

by Dr. Richard Raines

This article is the first in a series to introduce the Information Assurance/Information Operations (IA/IO) professional community to the capabilities of an Air Force and Department of Defense (DoD) educational and research resource, the Air Force Institute of Technology (AFIT). Specifically, this ongoing series will introduce the mission, academic, and research programs of AFIT's Center for Information Security Education and Research (CISER) and will provide contact information for inquiries. Later articles will highlight the ongoing research efforts of CISER faculty and students. From time to time, we will also spotlight graduates who make an impact on the DoD IA community.

Air Force Institute of Technology (AFIT)

AFIT, located on Wright Patterson Air Force Base, Fairborn, OH, grants graduate degrees and is accredited by The Higher Learning Commission of the North Central Association. In addition to institutional accreditation, the Accreditation Board for Engineering and Technology (ABET) accredits selected engineering programs within the Graduate School of Engineering and Management: Aeronautical Engineering, Astronautical Engineering, Computer Engineering, Electrical Engineering, Nuclear Engineering, and Systems Engineering. The Graduate School of Engineering and Management is the home of six academic departments supporting 25 scientific and management Master's degree programs and 15 scientific doctoral programs. The AFIT faculty comprises a nearly 50/50 mix between active duty military members and DoD civilians. This mixture ensures long term continuity through civilian faculty combined with current operational experience through military faculty members. Nearly 98% of the faculty holds doctorate degrees. The AFIT student body comprises DoD officers, enlisted personnel, civilians, non DoD US citizens, and international officers from Allied nations.

AFIT's location offers unique opportunities for faculty and students by providing ready access to IA facilities and researchers at the Air Force Research Laboratory (AFRL), the Air Force Materiel Command (AFMC), and the National Air and Space Intelligence Center (NASIC). The CISER faculty has long standing research relationships with each organization and with others not located at Wright Patterson. These relationships provide unique opportunities for student research, intern placement, and post-graduation employment. Research is an integral part of the AFIT educational experience, as all students are required to complete a Master's thesis or doctoral dissertation. Defense focused research is achieved through sponsorship by organizations of the DoD and the federal government. Currently, 95% of AFIT Master's theses are sponsored.

Center for Information Security Education and Research (CISER)

AFIT and CISER are forward-looking institutions, responsive to the changing educational needs of the Air Force, the DoD, and the federal government. The CISER was designated as an National Security Agency (NSA) National Center of Academic Excellence in Information Assurance Education (CAE/IAE) in 2002 and recertified in 2005 by the NSA and the Department of Homeland Security. In 2005, we also received a national CyberCorp Institution status from the National Science Foundation. Our foundational IA curriculum, established in 1995, is continually updated to maintain its currency and relevance as technological advances promote change.

Distinguished Review Board

Our graduate IA program is designed to support one of the federal government's and DoD's critical missions—Computer Network Operations (CNO). As DoD component element missions require rapid deployment and response on a global scale, our graduates must understand the technical and managerial roles associated with these complex IA mission requirements. To ensure that our educational program prepares graduates to meet the needs of the federal government, an external Distinguished Review Board (DRB) of IA experts and senior leaders oversees program direction. This DRB is chaired by Brig Gen Kimber McKenzie, Vice Commander of the 8th Air Force, and has a permanent member in Mr. Tony Sager, the Senior Executive Academic Liaison of the National Security Agency (NSA). Additional DRB members include: Col David Watt and Col David Nicholls, Commander and Vice Commander, respectively, of the Air Force Information Warfare Center; COL Carl Hunt of the Joint Task Force Global Network Operations; Mr. Alan Paller, Founder and Director of Research at the SANS Institute; Mr. Lance Spitzner, Founder of the Honeynet Alliance; Dr. Todd Stewart, Program Director for International and Homeland Security at the Ohio State University; and Mr. Will Janssen, a member of NSA's Senior Executive Service and an expert in IA. The DRB meets semiannually at AFIT to directly interface with CISER faculty and IA students. The DRB solicits feedback on the quality of course instruction, the focus and conduct of research, and the adequacy of laboratory and student support resources.

Graduate IA Curriculum

The resident Master's program, 48 quarter credit hours in IA, offers a unique blend of theory and practical application. By combining these two aspects, this program ensures that our graduates are prepared to meet the unique technical challenges posed by their gaining government employer and organizational missions. We believe that a solid theoretical foundation in IA is obtained through our classroom environment and interaction with our IA faculty, who possess years of practical experience. However, classroom theory is incomplete without laboratory application. We also feel that extensive "hands on" educational experiences are critical to promote learning.

Our curriculum includes computer and network forensics, biometrics, cyber operations, the protection of application software, formal analysis of protection systems, and the use of honeypots and honeynets to discover and counter threats to our computing and information network infrastructure. Two of our most popular subject areas, cyber forensics and cyber defense and exploitation, are highlighted.

Our Cyber Forensics course is an elective and examines the role of computer and network forensics in IO. Students gain insight into how computers are used in crime and the digital evidence that is available in a computer related investigation. Topics include the legal ramifications of evidence gathering, chain of custody, and methods for evidence preservation, identification, extraction, documentation, and interpretation and the tools available to perform this work. Student learning is enhanced through laboratory experiments that use a state of the art commercially available forensics tool, EnCase. Laboratory experiments examine how information can be hidden and extracted from a wide range of media from hard disks to pen drives. Students are also exposed to and asked to analyze the limitations associated with forensics tools and how these tools can be subverted.

Two courses comprise our cyber defense and exploitation curriculum. In the first, students use NSA Security Recommendation Guides to understand not only the potential cyber threat but also possible mitigation techniques and procedures. Students work in teams to harden network services using Public Key Infrastructure (PKI) and Secure Internet Protocol (IPSEC) procedures. The capstone of this two course sequence permits students to apply the theory and techniques learned in the previous course by participating in the annual Cyber Defense eXercise (CDX), sponsored by NSA. Using our dedicated Cyber Defense Network (CDN), students defend the CDN against cyber attacks launched by NSA Red team personnel. The CDX allows both undergraduate and graduate students at the service academies and AFIT to gain real life experience in protecting critical computing resources. For a period of five days, while the CDN suffers a variety of network infrastructure attacks, students must manage the network, thwart attacks, and maintain service availability to end users. This exercise provides powerful hands on learning experiences for the students. AFIT's team received the best scores in the 2003, 2004, and 2005 CDX competition in the graduate school division—a testimony to both the quality of our graduates and the strength of our program. At the time of this writing, the results of the 2005 CDX were not released.

Certificate Programs in IA

We offer two certificate programs in IA under the umbrella of the Committee on National Security Systems (CNSS). These programs can be taken as part of a Master's program or as stand alone programs. Students completing a set of required courses are eligible to receive the Certificate of Information Systems Security Professional (CISSP) under the National Security Telecommunications and Information Systems Security (NSTISSI) National Training Standard No. 4011 and the Certificate for Senior System Managers under the Committee of National Security Systems Instruction (CNSSI) No. 4012.

Graduate Research in IA

As previously mentioned, the CISER conducts defense focused research at the Master's and PhD levels. Our goal is to achieve 100% sponsorship through DoD organizations. We currently have strong research ties with the Anti Tamper Software Protection Initiative Technology Office of AFRL, the NSA, the Air Force Information Warfare Center (AFIWC), and the Air Force Communications Agency (AFCA). The CISER conducts both classified and unclassified research. Faculty and students hold security clearances capable of supporting research at the Top Secret level. The CISER faculty possesses a wealth of knowledge and experience in communications, networking, and information security gained through DoD operational assignments before joining the faculty. Recent research topics include extensive investigations into the vulnerabilities of IEEE 802.11 and Bluetooth networks, interference characteristics of ultra wideband systems on third generation communication systems, wireless traffic analysis, steganography and steganalysis, Internet Protocol Version 6 (IPv6) capabilities and security limitations, Intrusion Detection System (IDA) exploitation and evasion, security in remote sensor networks, and routing security in ad hoc communication networks. Highlights from specific research efforts will appear in subsequent articles. ■

For further information, please contact:

Dr. Rick Raines
Director, CISER
richard.raines@afit.edu
DSN: 785-6565, ext 4280
Comm: 937/255-6565, ext 4278

Mrs. Stacey Johnston
Program Coordinator, CISER
stacey.johnston@afit.edu
DSN: 785-3636
Comm: 937/255-3636, ext 4602

About the Author

Dr. Richard Raines

Dr. Richard "Rick" Raines is the Director of the CISER at the AFIT. Dr. Raines holds a BS degree in Electrical Engineering from the Florida State University, an MS in Computer Engineering from AFIT, and a PhD in Electrical Engineering from Virginia Tech. He teaches and conducts research in of information security and global communications.

IA Events

The 6th annual Institute of Electrical & Electronics Engineers (IEEE) Information Assurance Workshop (IAW) was held June 15–17 at the Thayer Hotel at the US Military Academy, West Point, NY. The conference featured research by academic institutions focusing on Information Assurance (IA) studies. Researchers from all over the globe came to present their research papers on cutting-edge technologies and groundbreaking tactics. Among the schools represented were Indiana University; Georgia Tech; Purdue University; Mississippi State University; the School of Information Systems at Curtin University, Perth, Western Australia; the University of Idaho; and many more. The Information Assurance Technology Analysis Center (IATAC) reviews IA technologies, such as those presented at this conference, to explore emerging technologies several years before they are made commercially available.

For the second year in a row, a focus was Honeynet Technologies, and new to the 2005 conference were the Biometrics and Security Data Visualization tracks. Papers were presented on detecting honeypots, knowledge-sharing honeynets, performance and impact to fingerprint recognition systems, image-compression algorithms for fingerprint and face recognition, real-time and forensic network data analysis using visualization, visualization techniques for intrusion identification, and visualizing network data. Other topics included papers on Intrusion Detection Systems (IDS), Wireless Technologies, IA Practices, and Data Protection. The papers also included wireless replication attacks on random key pre-dist schemes for wireless sensor networks, wireless policy for sensitive organizations, and reverse-code engineering the Bagle virus. Conference proceedings can be ordered from the IEEE Web site, http://www.ieee.org, using ISBN 0-7803-9290-6.

The award for the best paper, *Towards a Third Generation Data Capture Architecture for Honeynets*, was presented to Edward Balas and Camilo Viecco from Indiana University. This paper describes how a honeynet can be used as a research tool for network operators, to see how a hacker works on a live network, and how the next-generation honeynet will create a unified data model. An upcoming issue of the *IAnewsletter* will feature some of the various papers that were presented during the conference. Topics to be covered include spammers' behaviors through honeypots and safe key renewal on trusted devices.

Colonel Carl Hunt delivered a presentation on Net Force Maneuver, a NetOps construct. The objective of Net Force Maneuver is to draw adversaries from mission-critical systems to learn about their techniques capabilities, a topic of considerable interest at the conference.

The week concluded with a tour of the West Point IA laboratory. The Information Warfare Analysis and Research (IWAR) laboratory is the facility at which Information Technology and Operations Center (ITOC) staff and students conduct research and analysis in a realistic environment. Staff and students use tools for computer penetration and exploitation and can experiment with and use malicious software to learn how these applications work in a real-world network environment.

Please check the IEEE Information Assurance Workshop Web site: http://www.itoc.usma.edu/workshop for more information about next year's conference. ■

letters to the director

"I read these great articles in the IAnewsletter all the time. What if I have a topic that I would like to write on?"

As you know, the *IAnewsletter* highlights current Information Assurance (IA) initiatives within the US Department of Defense, industry, academia, and Research & Development (R&D) communities. This quarterly publication, distributed to more than 7,000 IA and Information Operations (IO) professionals, features timely articles from the IA community. Articles are being solicited constantly from Subject Matter Experts (SMEs) in such organizations as the Office of the Secretary of Defense (OSD)/Joint Staff, Services, Combatant Commands, Agencies, Government R&D Labs, academia, and industry. We recently received a request to see an article related to SPAM. We reached out to our SMEs, and, as you may have noticed, we have included an article on the topic in this edition of the *IAnewsletter*. Typical articles in the past have included technical papers, overviews of emerging or established IO technologies, articles from the perspective of the warfighter "in the trenches," and lessons learned. However, these are not the sole topics covered by the newsletter and should not limit your own choice of subject matter.

If you have written or would like to write an article that you think may be of interest to the IA community and would like us to consider it for publication, please submit the article *via* e-mail to iatac@dtic.mil. Please ensure that the article is between 1,500–3,000 words and has a working title of six words or less. The article should be clear, concise, and as non-technical as possible to ensure the widest understanding and interest among our readers. All submissions should also include a completed "Article Submission Instructions" form, available on our Web site, http://iac.dtic.mil/iatac/download/article_instructions.pdf; the authors biography; and approval from the Public Affairs Office. It is imperative that all articles be kept Unclassified, Distribution A: Approved for Public Release, so that we can ensure the widest possible distribution.

For more information, visit our Web site at http://iac.dtic.mil/iatac/IA_newsletter.html, call us at 703/289-5454, or e-mail us at iatac@dtic.mil ■

A Honeypot for the Exploration of Spammers' Behavior

by Guido Schryen

Spam has become one of the most annoying and costly phenomenon on the Internet. Valid e-mail addresses are among the most valuable resources of spammers, but little is known about the methods by which spammers collect and harvest addresses. Spammers' capabilities and interest in carefully directed, consumer-oriented marketing have not yet been explored. Gaining insight into spammers' ways of obtaining and misusing e-mail addresses is useful in many ways; *e.g.*, for assessing the effectiveness of techniques that obscure addresses and the usefulness and necessity of hiding e-mail addresses on the Internet. This paper presents a spam honeypot project in progress that addresses these issues by systematically placing e-mail addresses on the Internet and analyzing received e-mails.

The Threat

Spam is generally recognized as an increasingly disturbing and costly issue for electronic business and Internet traffic. Companies, non-profit organizations, and individuals receive this type of e-mail to such an extent that the issue has certainly gone beyond that which is merely "annoying." Symantec reports that, in scanning 100 billion e-mails, the percentage of spam e-mails reached 69% in January 2005 but decreased to 60% in May. [1] MessageLabs announced that the average global ratio of spam was nearly 70% in May 2005, although the sample of e-mails inspected was much smaller, comprising some one million per day. [2] The content of spammers' e-mails covers a broad range of topics:

- Offering or advertising general goods and services, such as devices, investigative services, clothing, and makeup (21% of all e-mails categorized as spam)
- Containing references or offerings related to money, the stock market, or other financial "opportunities" (19%)
- Containing or refering to products or services intended for persons above the age of 18 (10%)
- Offering or advertising health-related products and services (13%) [1]

The increased payload of networks and e-mail servers and the demand on employees' time and attention are not the only harmful effects of spam e-mails. Fraudulent messages; *e.g.*, e-mails that appear to be from a well-known company but are not—also known as "brand spoofing" or "phishing" e-mails—are often used to trick users into revealing personal information, such as e-mail addresses, financial information, and passwords (7%). Furthermore, viruses, worms, and Trojan horses (opening backdoors for botnets using the infected computer as a spam client) are distributed over the Internet. The total economic damage caused by spam e-mails is estimated at several billion dollars. [3]

This central economic aspect has motivated anti-spam activities embracing many facets: national laws and international regulations (about which Hintz [4] provides a good overview); organizational provisions, including abuse systems (*e.g.*, http://spam.abuse.net/) and lists of suspicious domains and IP numbers; and technical solutions that mainly apply blocking, filtering, or authenticating mechanisms. [5] Statistics and e-mail users' daily experience show that the spam problem is far from being solved, and it is only by applying technical anti-spam that the collapse of our Internet e-mail system has been prevented.

Implementing honeypots and honeynets has emerged as a solution [6, 7], along with these mainstream efforts to analyze spammers' behaviour or to even attack them. The honeypot presented here contributes to this field by setting up a technical environment that analyzes where spammers get their e-mail addresses and how they exploit them—or if they simply use any harvested e-mail address. (A more detailed presentation of the honeypot project can be found in Schryen, [8]).

Motivation and Goals

Valid e-mail addresses are among the most valuable resources of spammers, and identifying address sources and the procedures used by spammers to exploit them is crucial to preventing spammers from getting addresses and misusing them. It is widely known that, besides generating addresses with brute-force mechanisms, spammers get valid e-mail addresses by harvesting the Internet or, illegally, from organizations. Some Address Obscuring

Techniques (AOTs) that restrict the availability and usability of e-mail addresses have been proposed: As early as 1997, Hall [9] described e-mail channels, and in 2003, Ioannidis [10] presented a policy for encapsulating single-purpose addresses. Many users also use temporary addresses and dispose of them when they feel that the spam quotient has become too high.

Gaining insight into spammers' ways of obtaining and misusing e-mail addresses is useful in many ways:

- Assessing the effectiveness of AOTs and input for their improvement
- Identifiying spammers to lead to their prosecution
- Assessing the usefulness and necessity of hiding e-mail addresses on the Internet
- Discovering specific marketing and addressing activities

The last item, above, focuses on the quality of e-mail addresses. Spammers are known to collect as many valid e-mail addresses as possible, but little is known about spammers' capabilities and interest in carefully directed, consumer-oriented marketing. A taxonomy of quality for e-mail addresses is shown in Figure 1.

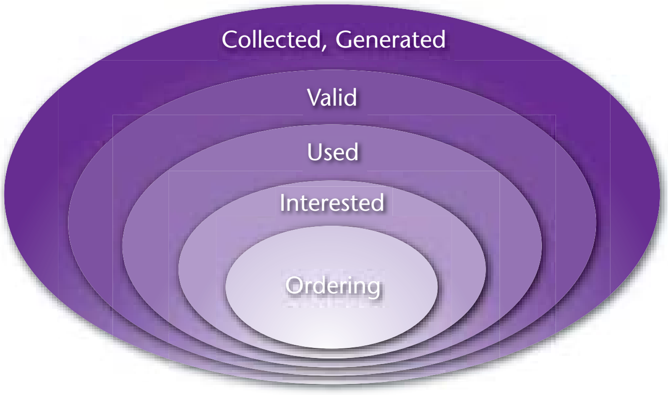


Figure 1: Taxonomy of E-mail Addresses

The inner ellipses are more valuable for spammers than the outer ones because of losses caused by non-selective advertising. Only a portion of collected or generated e-mail addresses are valid ones, *i.e.*, e-mails addressed to non-valid ones are refused by the addressee's host because these mailboxes do not exist. Valid ones can be divided into addresses actually in use and those that are no longer accessed and thus useless for spammers. A way to distinguish between the two is provided by an "opt-out" option included in some spam e-mails; however, when this option is used incautiously by the spam recipient, it indicates that the address is in use. Spammers will go even further and adopt physical marketing strategies using knowledge about consumer-specific interests and behaviour; *e.g.*, an Internet user actively participating in a German discussion group that focuses on medical products is presumably interested in offers of medical products in the German language. The innermost ellipse contains e-mail addresses of users who buy products and thus from whom the spammer profits.

The goal of the honeypot is to (1) penetrate spammers' behavior in harvesting e-mail addresses from Internet services, such as newsgroups and the Web, and (2) to discover the extent to which spammers have already shifted from simply employing e-mail addresses in use towards acquiring addresses of users likely to be interested in specific marketing.

Conceptual Framework

To cover a broad range of locations that are attractive to spammers for harvesting e-mail addresses, it is necessary to inspect many Internet services. Integrated into this honeypot are newsletters and mailing lists, Web pages, Web chats, chats, and the Usenet in which e-mail addresses are placed. There are many more ways in which spammers can get e-mail addresses [11] that have not yet been covered. This is simply caused by the limited resources of the project, which is currently not funded.

To detect linguistic and regional particularities, each medium is divided into those that are oriented to the German language and those that are US based. This furnishes a second, desirable dimension in that it renders the study readily extensible to other languages and regions. To inspect spammers' behavior regarding specific marketing activities, a third dimension of the survey focuses on the topic of the Internet service. For example, Web pages and newsletters and mailing lists are divided into those ruled by an individual, a discussion board, a greeting-card service, *etc.*, in which the topics are grouped by types of administration, content, connection, context, and commerce. (For a complete list of topics, see Schryen, [8]) It should be noted that topics are service specific. Figure 2 shows the classification of Internet locations as used in the empirical study. Each type of location is represented by a cube, each cube contains three locations (a location is a specific Web site or a specific newsletter), each location gets four addresses (de-, com-, net-, and org-address), and for each cube 12 e-mail addresses must be reserved. This procedure makes it possible to detect if the top-level domain of an e-mail address is relevant. So far, German and US newsletters and mailing lists and Web pages have been addressed, *i.e.* the number of e-mail addresses placed for getting harvested is almost 2*2*36*12, which is 1728. Of course, no e-mail address must be seeded more than once.

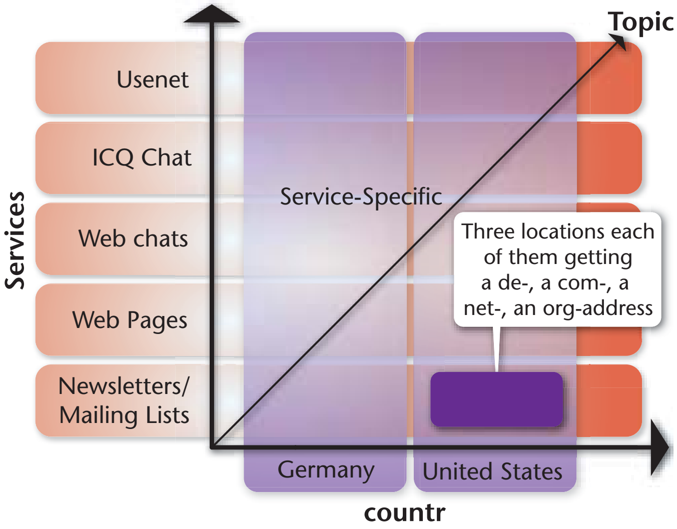


Figure 2: Classification of Internet Locations

Implementation

A mail server has been set up, charlie.winfor.rwth-aachen.de, and three domains have been reserved, wforasp.com, wforasp.net, and wforasp.org, to cover the e-mail addresses of four top-level domains. All e-mails addressed to these domains are directed to this mail server. As thousands of e-mail addresses had to be created, they were automatically generated by a random generator for the user part of the addresses. To prevent e-mail addresses from being guessed or generated with brute-force attacks, it is necessary to define them randomly and to give them an appropriate number of characters. An example of an e-mail addresss created this way is wasp10208@wforasp.com. The Internet locations serving as lures were chosen manually, just as the placement of the e-mail addresses had to be done manually. As soon as an e-mail address is spread, its location and activation date is stored.

All incoming e-mails are classified into regular e-mails (ham e-mails), such as regular newsletters or the like that contain comments from users of discussion forums, and spam e-mails. This procedure is currently mainly executed by humans but supported by a mail parser written in Hypertext Preprocessor (PHP), which uses an increasing white list containing pairs of recipient-addresses, Internet Protocol (IP) entries: each time a host was manually assessed as qualified to send an e-mail to the recipient address, its IP number was linked to this e-mail address and stored in the white list. A second task of the mail parser is to decompose each incoming e-mail—all entries of the header and the content are analyzed, as is the Multipurpose Internet Mail Extensions (MIME) structure of the body. (A detailed description of the relational data model on which the procedure is based is beyond the scope of this paper.) Next, the e-mails' elements are stored in the Structured Query Language MySql database broken down into spam and ham e-mails. The database is intended to be used by data-mining tools and (simpler) statistical analyzers. Figure 3 provides a survey of the implementation infrastructure.

First Empirical Results

In total, 15,178 ham e-mails and 8,189 spam e-mails have been recorded by our mail server. Because of the very early stage of the project, the results presented here are preliminary; however, some facts are worth mentioning:

- No spam has been sent to addresses that were used for subscribing German newsletters/mailing lists.
- Only a few spam e-mails have been received by way of US newsletter/mailing list subscription. The few are all due to administration topics.
- Not surprisingly, many more spam e-mails arise from placements on web pages. Interestingly, German web pages were responsible for only a third of the number of spam e-mails that are due to US web pages. Net-addresses seem to be of greater interest to spammers than de- and org-addresses independently of any country; on US web sites com-addresses have been even more used by spammers.

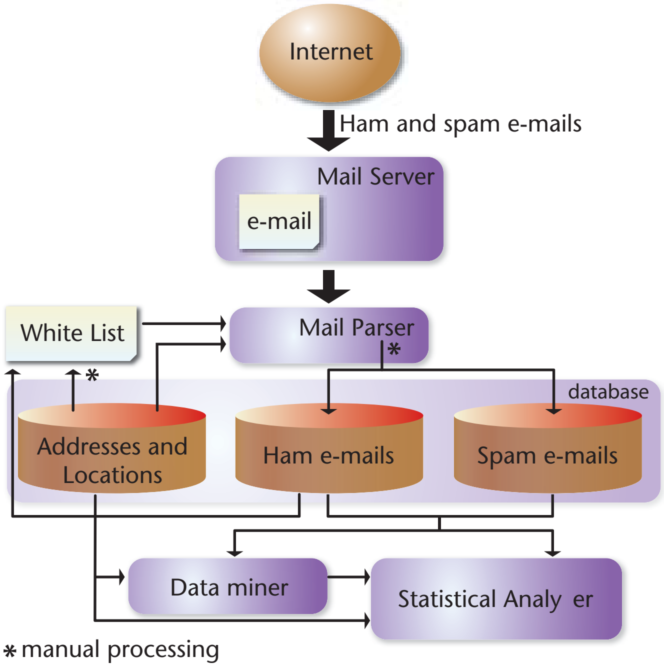


Figure 3: Infrastructure of the E-mail Honeypot Environment

Summary and Outlook

Spammers are known to collect as many valid e-mail addresses as possible, but little is known about spammers' capabilities and interest in carefully directed, consumer-oriented marketing. Gaining insight into spammers' ways of obtaining and misusing e-mail addresses is useful for

- Assessing the effectiveness of AOTs
- As input for the improvement of AOTs
- For identifying spammers leading to their prosecution
- For assessing the usefulness and necessity of hiding e-mail addresses on the Internet
- For discovering specific marketing and addressing activities

This article sketches a honeypot to penetrate spammers' behavior in harvesting e-mail addresses from Internet services, such as newsgroups and the Web, and in discovering the extent to which spammers have already shifted from simply employing e-mail addresses already in use toward acquiring addresses of users likely to be interested in specific marketing offers. The honeypot's conceptual framework classifies Internet locations as used in the empirical study using three dimensions: Internet services, (*e.g.*, the Usenet, Web pages, newsletters); service-specific topics such as education, infotainment, auctions; and countries. Each location gets four addresses (de-, com-, net-, and org-address), which permits the researcher to detect if the top-level domain of an e-mail address is relevant for spammers. When e-mails arrive at the honeypot's mail server, they are classified into spam and ham e-mails (regular e-mails), decomposed by a parser, and stored in a database that is intended to be used by data-mining tools and (simpler) statistical analyzers. Preliminary results of the honeypot study are presented, which show that no spam has been sent to addresses that were used for subscription to German newsletters and mailing lists, that only a few spam e-mails have been received due to US newsletter and mailing-list subscriptions, that many more spam e-mails arise from placements on Web pages, and that net-as well as com-addresses seem to be of particular interest to spammers.

The project is at an early stage. More services and countries remain to be integrated, more data must be collected for more reliable results, and a time-series analysis must be applied. Another avenue that needs to be explored is the functional; *i.e.*, the application of data-mining procedures and statistical procedures aiming at detecting differences between spam and ham e-mails. These results can be used to improve spam filters.

The experiences gained from the prototypic honeypot implementation can be used to develop a general blueprint for further honeypots that explore spammers' behaviour and the effectiveness of AOTs. Depending on funding, software tools will be included to enable a semi-automated setup and utilization of future honeypots. ■

References

[1] Symantec, Spam statistics, http://www.symantec.com/region/de/PressCenter/spam.html [Accessed 04/01/05].

[2] MessageLabs, Email Threats, http://www.messagelabs.com/emailthreats/default.asp [Accessed 04/01/05].

[3] OECD, Background Paper For The OECD Workshop On Spam, 2003.

[4] Hintz T., Opt-In vs. Opt-Out Legislation, http://notebook.ifas.ufl.edu/spam/Legislation.htm [Accessed 04/01/05].

[5] Schryen, G, Effektivität von Loesungsansaetzen zur Bekaempfung von Spam, Wirtschaftsinformatik 46 (2004) 4, pp. 281–288. (English version is not published but is available from the author.)

[6] The Honeynet Project. http://honeynet.org. [Accessed 04/01/05].

[7] Project Honey Pot. http://www.projecthoneypot.org. [Accessed 04/01/05].

[8] Schryen, G., An e-mail honeypot addressing spammers' behavior in collecting and applying addresses. Proceedings of the 6th IEEE Information Assurance Workshop, West Point, pp. 37–41.

[9] Hall, R., Channels: Avoiding Unwanted Electronic Mail. Proceedings DIMACS Symposium on Network Threats DIMACS, 1996.

[10] Ionnadis, J, Fighting Spam by Encapsulating Policy in Email Addresses. Network and Distributed System Security Symposium (NDSS'03), 2003.

[11] Raz, U., How do spammers harvest email addresses? http://www.private.org.il/harvest.html [Accessed 04/01/05]

Acknowledgements

The setup of the honeypot was strongly supported by Reimar Hoven. The classification of incoming e-mails had to be performed manually, to which task Stephan Hoppe dedicated much time. Many thanks are also due to Jan Herstell and to Katrin Ungeheuer for proofreading.

About the Author

Guido Schryen

Mr. Guido Schryen graduated from the RWTH Aachen University (Germany), where he earned a Masters' degrees in Computer Science and in Operations Research. He received his PhD from the Faculty of Business Administration and Economics of RWTH Aachen University where he now holds a postdoctoral position. His current research activities focus on Internet security and anti-spam measures. He may be reached at schryen@winfor.rwth-aachen.de.

Taxonomy Development Methodology

by Gopal Swamy

Editor's Note: *The Total Electronic Migration System (TEMS) taxonomy-development effort provides a comprehensive thesaurus of scientific and technical terms relating to Information Assurance (IA). Since this thesaurus emphasizes relationships in terms and associations among and across similar documents, IATAC staff analysts will be able to "discover" related information without having to know specifically what they are looking for in advance. This "tree view" of IA terminology augments the word-search capabilities of TEMS and provides the IATAC staff with a powerful tool to conduct more in-depth analyses and to respond quickly to the information-security requirements of the community.*

This article describes a high-level taxonomy framework and a more project-specific methodology that details the process used to create, refine, and publish a taxonomy as well as more detailed steps currently being followed at IATAC in order to create the IATAC taxonomy used to categorize the documents in the IATAC repository. The individual steps of the framework are described at a high level followed by a specific IATAC methodology with corresponding activities explained in detail.

A Taxonomy Development Framework

Useful taxonomies are created through a phased approach that drives value realization by implementing and iteratively improving taxonomies over time. The High-Level Taxonomy Development Framework illustrated in Figure 1, outlines the phases through which taxonomy development progresses, the key outputs of each phase, and the process by which the taxonomy moves from value identification through value delivery. Using this framework as the basis for designing a specific methodology creates intuitive, accurate, and relevant taxonomies and maximizes the value derived.

- **Design Phase**—The design phase set the mission, goals, and success targets that development of taxonomy is designed to achieve. Further, this phase details resource needs by defining the taxonomy team and establishes dependencies that must be met in order to support the effort. Finally, this phase prepares a Proof of Concept Taxonomy in preparation for the Testing phase. All analysis that has been performed up to this point should be consolidated and examined in order to assess any impact on subsequent phases. Ultimately, this preparatory phase paves the way for the taxonomy to be tested, applied and maintained and for value from the development of the taxonomy to be delivered.

- **Test Phase**—The objective of the Test phase is to validate the high-level taxonomy architecture and proof of concept taxonomy by conducting inter-

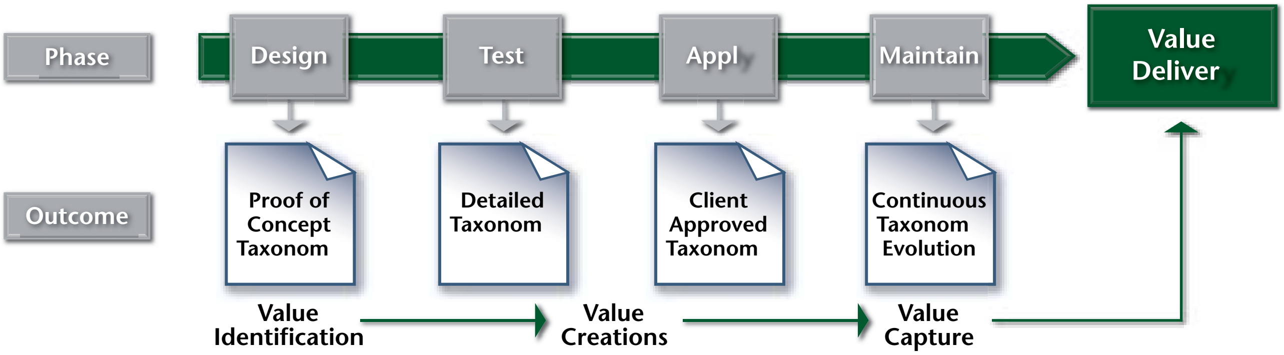


Figure 1. High-Level Taxonomy Development Framework

views, developing use cases and leveraging these artifacts to ensure that the taxonomy that is being developed meets the needs of users and allows information and data to be categorized so that it can be located quickly and easily. It is key to ensure that no important content has been missed, and that the level of detail within and across the dimensions is appropriate and consistent. The result of the testing phase is the creation of low-level, Detailed Taxonomy that can be approved, applied and maintained by the client.

- **Apply Phase**—The Apply phase consists of the final approval and roll out of the taxonomy. This taxonomy will be used to categorize content.
- **Maintain Phase**—The Maintain phase contains a set of tasks that, when performed, allow the taxonomy team to enhance the taxonomy and keep it up to date. Taxonomy development and maintenance is an iterative process that must be performed at regular intervals in order for an agency or enterprise to continuously recognize the benefits of taxonomy development.

A Project-Specific Methodology— Taxonomy Development at IATAC

The Taxonomy Development team began the process of taxonomy development by calling on IATAC Subject Matter Experts (SMEs) to validate the accuracy and relevance of the developing taxonomy. This validation is being performed by SMEs manually reviewing taxonomy categories and comparing these categories to already existing thesauruses, vocabulary lists, and other taxonomy-related artifacts. Taxonomies are also being validated based on the number of documents that were placed into each category through cursory examination of the documents in each category.

As the project proceeded, the team evaluated the existing commercial-off-the-shelf (COTS) classification products and elected to use Convera Categorization and Dynamic Classification software. This software includes metric-gathering and presentation capabilities that enabled the team to more precisely refine the taxonomy framework detailed above. This produced a TEMS and IATAC-specific methodology described in Figure 2 that is divided into phases with specific goals, and contains structured activities that help create phase-level deliverables. These deliverables serve as checkpoints to ensure that taxonomy creation at IATAC follow a defined path and are reviewed at the end points of each phase.

Design and Test Phase

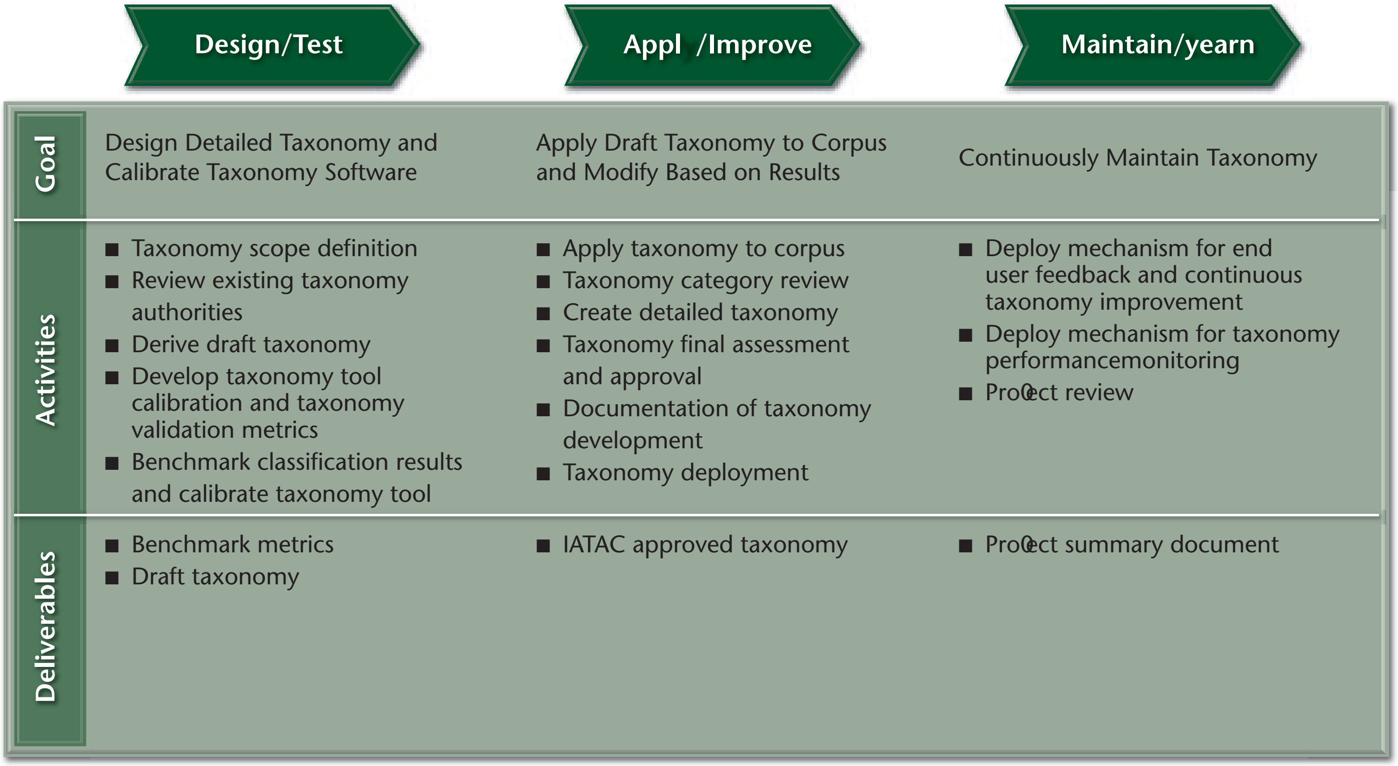
The Design and Test phase establishes the mission, goals, and success targets that taxonomy development is designed to achieve. This phase explains the required resources by defining and identifying the dependencies that are to be met to support the effort. This initial phase paves the way for the taxonomy to be tested, applied, and maintained, so that value can be derived from it by providing a client with intuitive, logical categories and subcategories.

Specifically, the objective of this phase is to create and validate the draft taxonomy by using the Convera software; in this case, to ensure that the developing taxonomy fulfills the requirements of the IATAC SMEs.

Outputs of the Design and Test phase are benchmark metrics and calibrated taxonomy software that help ensure when the software is used to crawl document collections, the categorization results permit end users to find information quickly and easily. Finally, this phase produces a Draft Taxonomy in anticipation of the Apply and Improve phase.

Design and Test Phase Activities

- **Taxonomy Domain and Scope Definition**— Defining a taxonomy's domain and scope requires that several basic questions be asked and answered, as shown in Table 1. (See next page.)



	Design/Test	Appl /Improve	Maintain/yearn
Goal	Design Detailed Taxonomy and Calibrate Taxonomy Software	Apply Draft Taxonomy to Corpus and Modify Based on Results	Continuously Maintain Taxonomy
Activities	■ Taxonomy scope definition ■ Review existing taxonomy authorities ■ Derive draft taxonomy ■ Develop taxonomy tool calibration and taxonomy validation metrics ■ Benchmark classification results and calibrate taxonomy tool	■ Apply taxonomy to corpus ■ Taxonomy category review ■ Create detailed taxonomy ■ Taxonomy final assessment and approval ■ Documentation of taxonomy development ■ Taxonomy deployment	■ Deploy mechanism for end user feedback and continuous taxonomy improvement ■ Deploy mechanism for taxonomy performancemonitoring ■ Project review
Deliverables	■ Benchmark metrics ■ Draft taxonomy	■ IATAC approved taxonomy	■ Project summary document

Figure 2. IATAC-specific Methodology

- **Review Existing Taxonomy Authorities**—Before beginning taxonomy creation, the team considered all existing, relevant classification schemes and controlled vocabularies to determine if these artifacts should be incorporated into the developing taxonomy. The team worked with the IATAC SMEs to make use of thesauruses and existing taxonomies. Failure to glean relevant categories and relationships already established within these taxonomies would have increased the time required to develop the taxonomy.

- **Derive Draft Taxonomy**—This step includes discovering, extracting, and documenting all categories and subcategories that are relevant to the subject domain. Derivation of the categories and subcategories was performed by SMEs who used domain knowledge and existing taxonomy authorities to assemble a list of categories to construct a draft taxonomy. By working with SMEs, the team solicited the participation of the individuals who have the appropriate domain knowledge and can accurately represent the requirements of IATAC. When developing the draft taxonomy, the team ensured that categories were descriptive enough to be both meaningful and unique; ensuring that cate-

Table 1. Taxonomy Scope and Definition

Taxonomy Scope and Definition Questions	Answers
What is the subject domain that the taxonomy will cover?	Subject domains cover content specific to the IATAC.
How will the taxonomy be used? For what purpose?	Taxonomy will be used in conjunction with a GUI to provide users an easy and intuitive way to locate the information they need.
Who are the users of the taxonomy?	Taxonomy users are IATAC staff and its affiliates.
Who are the members of the team who will collaborate to create the taxonomy?	The Taxonomy team's experts collaborate with IATAC SMEs and follow the methodology described in this document to create the taxonomies.
What are the dependencies? Does the content have metadata? What is the quality of the metadata?	Document metadata is being written and read by the Convera software. This will produce high-quality metadata that will enable end users to quickly and easily find and retrieve the information they seek.
What can be done in the project time frame? What percentage of time can resources dedicate to creation and maintenance?	Taxonomy efforts on a project are completed within a predetermined time frame, and all funds associated with taxonomy creation are used. The resources dedicated to taxonomy maintenance have yet to be determined.

gories reflect the documents they intend to classify. The draft taxonomy produced serves as the skeleton of the final, IATAC Approved Taxonomy and contains all high-level categories and subcategories into which the content falls.

- **Develop Taxonomy Software Calibration Metrics and Taxonomy Validation Values**—The team developed metrics to calibrate the Convera software so that categorizing of documents is accurate. Furthermore, the team also developed a set of values that are being used to gauge the validity of the taxonomy. These metrics and values are constantly examined enabling the team to possess a "living" set of information used throughout the taxonomy development and maintenance cycle. After initially implementing the taxonomy, this information will be used to enhance the taxonomy so that the value derived continues to increase over time.

- **Benchmark the Classification Results and Calibrate Taxonomy Software**—In an ideal world, SMEs would read and categorize every document in the IATAC corpus. However, because this effort is not scaleable, the team recognizes the need to rely on Convera software to perform the categorization of documents in order to save time and manual effort. The benchmarking and calibration activity permits the team to determine the differences between the categorization performed by the software and the ideal categorization that would be performed by SMEs if time and resources permitted.

  - To benchmark and calibrate the Convera software, SMEs gathered 50–100 documents that comprise a representative sample of the corpus and manually categorized them into categories defined in the draft taxonomy. These categorized documents and the categories in which they are placed were then recorded. The team is now using Convera software to categorize the same 50–100 documents using the same taxonomy as that of the manual categorization process. Once this is complete, a comparison will be made between the manual and automatic categorization processes, and any differences between the two are revealed.
  - After the benchmarking process, the team will determine the Precision and Recall metrics for the taxonomy categories and work with the SMEs to determine how the parameters of the Convera software can be modified to produce an automated categorization that closely follows, if not mirrors, the ideal manual categorization.
  - The calibration activity is an iterative process that is repeated until the SMEs are satisfied with the automated results. Once benchmarking and calibration are completed, the Apply and Improve Phase can begin.

- **Deliverable: Calibration Metrics**—Calculated values for the Calibration Metrics are captured for use in configuring the Convera software so that the automated categorization is as close as possible to an SME's manual categorization.

- **Deliverable: Draft Taxonomy**—The Design and Test phase culminates in the creation of a Draft Taxonomy, which serves as the starting point for the Client-Approved Taxonomy (IATAC Taxonomy) that will be deployed to provide the browsing structure for the Convera GUI.

Apply and Improve Phase

The Apply and Improve phase consists of applying the Draft Taxonomy to the IATAC corpus and modifying the taxonomy based on the results produced by the Convera software. IATAC SMEs evaluate a set of taxonomy values in order to develop and validate the IATAC taxonomy. The team then modifies the categorization parameters in the software and re-crawls the corpus, thereby producing a new set of taxonomy results and values. This process is reiterated until the SME is satisfied with the results. Finally, the taxonomy is approved by the team and deployed.

Apply and Improve Phase Activities

- **Apply Taxonomy to Corpus**—After the Draft Taxonomy is created and the Convera software has been calibrated, the team applies the Draft Taxonomy to the entire IATAC document set to test the accuracy and validity of the taxonomy. To do this, the team loads the Draft Taxonomy file into the software, points the software at the repository containing the client's documents, crawls the documents, and automatically inserts them into categories contained within the draft taxonomy. The Convera software also records categorization values allowing the team to use this data in the next steps to assess, modify, and eventually validate the taxonomy.

  - **Taxonomy Category Review**—After categorizing the documents, the taxonomy is examined, modified, and validated. Validating the draft taxonomy is performed through a category review for balance, breadth, and depth. Categories are reviewed in conjunction with their content to ensure that relationships between categories and content are logical and easy to understand, and that they meet the needs of end users while falling within the larger constraints of IATAC mission and goals. Categories are also assessed in terms of the amount of content they contain vs. other categories. Well-built taxonomies contain categories with similar amounts of content across taxonomy levels. In short, this step ensures that categories are neither overpopulated nor under populated. If categories are inconsistently populated, the team re-examines the taxonomy to determine if key areas have been combined or unnecessarily split up, and breaks these areas out or combines categories where relevant. Finally, a review of uncategorized documents is performed. This step highlights the requirement to analyze these documents, determine why they remain uncategorized, and devise steps to categorize them accurately. When necessary, the team also can add categories and refine rules for categorization within the Convera software.

  - The Taxonomy Category Review is an iterative process that continues until the SME is satisfied with the metrics produced by the Convera software. Ideally, these results show that the taxonomy is accurate, relevant, and appropriately broad and deep.

- **Create Detailed Taxonomy**—Through this activity, a modified, detailed taxonomy is created, which is then examined and improved through an iterative use of the Convera software as discussed in the previous step. Once sufficient changes to categories and subcategories are made, the taxonomy is captured and deemed the Detailed Taxonomy.

- **Taxonomy Final Assessment and Approval**—In this step, the team examines the taxonomy and conducts intensive testing by attempting to place and locate documents into the taxonomy to ensure that no content is incorrectly categorized or difficult to locate. This is a key point in the project methodology. The team works with stakeholders who participate in the taxonomy's development and with other stakeholders who can provide a fresh view into the taxonomy and content being categorized. By leveraging stakeholders who are familiar with the taxonomy as well as those who are not, the team ensures that the taxonomy is intuitive to all users and maintains consistency throughout the taxonomy generation process. Any minor changes are captured at this stage and reserved for implementing future iterations of the taxonomy. Significant problems with categorizing and locating documents indicate a problem in previous phases of the taxonomy development process and the time frames associated with taxonomy deployment are revisited. If the taxonomy meets the requirements of the SMEs and end users without significant problems, the taxonomy is approved by IATAC SMEs and is considered the IATAC Approved Taxonomy.

- **Documenting Taxonomy Development**—To ensure that key decisions and elements of the taxonomy are captured, the creation of the taxonomy development process is documented. This documentation serves as a record of the taxonomy's creation and is used when revising or redesigning the taxonomy. Important events and decisions—and the rationales and justifications for business decisions—are captured in the documentation for use in future IATAC taxonomy projects.

- **Taxonomy Deployment**—The Approved Taxonomy is rolled out and the documents are categorized accordingly.

- **Deliverable: An Approved Taxonomy**—The Apply and Improve phase culminates with examining and modifying the draft taxonomy until it meets the requirements of the IATAC SMEs. At that point, the taxonomy is officially approved and is considered the final, approved taxonomy. This taxonomy is deployed and used to provide the browsing structure for the Convera GUI used to browse and search for IATAC documents.

Maintain and Learn Phase

The Maintain and Learn phase contains tasks that, when performed, permit the team to keep the taxonomy current. Taxonomy development and maintenance is an iterative process that must be performed at regular intervals to enable an agency or enterprise to continuously recognize the benefits of taxonomy development.

Maintain and Learn Phase Activities

- **Mechanism for End-User Feedback and Taxonomy Improvement**—A formalized process is developed to report problems and issues in categorizing documents in the taxonomy and in locating documents based on the taxonomy. This process includes a mechanism for cataloging issues and feeds into the change-management process for implementing enhancements and upgrades to the IATAC Taxonomy.

- **Mechanism for Taxonomy Performance Monitoring**—Monitoring predefined, taxonomy related metrics enables the team to collect data on the taxonomy's effectiveness in categorizing information. Based on the reporting of key metrics (Convera-generated metrics, search logs, and direct user feedback), areas of the taxonomy may need to be altered. Over time, a client's information and data may also change significantly, thereby requiring the taxonomy to change significantly. The decision to significantly change or completely redesign the IATAC taxonomy is determined by an ongoing analysis of metrics and user feedback.

- **Project Review**—A review of the project charter, management, and change-management objectives is performed and revisions made for further taxonomy development. All created documentation is examined at this stage, and as a client's objectives and content change, new taxonomy projects can be scoped and designed as needed. The project-review activity culminates with a Project Summary document.

- **Deliverable: Project Summary Document**—The Project Summary Document includes (1) a brief summary of project goals, milestones, and relevant dates of significant events; (2) the finalized IATAC taxonomy; and (3) a description of activities and issues that the client should bear in mind after the initial implementation to maintain intuitive, accurate taxonomies. This document serves as a formal presentation and handoff of the taxonomies.

Taxonomy Metrics and Values

The team developed and is implementing two sets of metrics:

- **Calibration Metrics**—The team developed and uses a set of metrics to calibrate the Convera software. SMEs use these metrics to assess the similarity between the automated classification performed by the Convera software and the classification they themselves would perform if they were to manually categorize the documents.

- **Taxonomy Validation Values**—The team uses a set of values that are used to aid in the validation of the IATAC taxonomy.

Calibration Metrics

The Calibration Metrics developed and used are simple and straightforward and provide the team with a way to examine the automated taxonomy classification and ensure that documents are categorized by the taxonomy software just as they would be if categorized by SMEs.

The metrics, Precision and Recall, permit the team to analyze documents in various taxonomy categories and gauge the accuracy of the Convera software's categorization of documents. It is important to note that, strictly speaking, the size of the document corpus is irrelevant to calculating Precision and Recall ratios. However, in practice, larger corpuses decrease precision. Also, determining Precision and Recall requires knowledge of categorization accuracy from outside the Convera software; hence, the involvement of SMEs. The Convera software can never know which documents are truly categorized "correctly."

- **Precision**—End users of the applications search for documents by entering terms into a search field or by browsing through categories and subcategories defined in the taxonomies. The term Precision compares the number of documents located in a taxonomy category or subcategory that are correctly placed with the total number of documents placed in the category. Correctly placed documents are referred to as True Positives, while the sum total of all documents located in each category is defined as the Results Set. Incorrectly placed documents are False Positives. With these definitions in mind, the Precision metric is defined as the number of True Positives divided by the Results Set, as follows:

  Precision = Number of True Positives/Results Set

  The Precision metric enables the team to determine the precision of the Convera software's categorization of documents. As the ratio approaches 1.0, the overlap between documents that belong in the taxonomy category and the documents that are placed in the taxonomy category increases. As the ratio approaches 0.0, that overlap decreases The team is looking for a ratio close to 1.0, which indicates the Convera software is placing documents accurately into categories. If the ratio is low, the team makes modifications to the parameters that govern the automatic classification of the documents.

- **Recall**—Recall indicates how many documents that should be placed in a category or sub-category are actually placed into that category or subcategory. The number of documents that should be placed in a category or sub-category is defined as the Ideal Result Set. With this in mind, the Recall metric is defined as the number of True Positives divided by the Ideal Results Set, as follows:

  Recall = Number of True Positives/Ideal Result Set

  The Recall ratio enables the team to establish the relationship between the number of missing documents in a category and the correctly categorized documents in that category. As the Recall ratio approaches 1.0, the number of missing documents decreases. As the ratio approaches 0.0, the number of missing documents increases. The team is looking for a ratio close to 1.0, which indicates the Convera software is placing only the documents that truly belong in a given category into that category. As stated above, if the ratio is low, the team makes modifications to the parameters that govern the automatic classification of the documents.

Taxonomy Validation Values

Convera software can be used to examine the categories and subcategories within the IATAC taxonomy to perform taxonomy validation.

Table 2 (see next page) contains a list of values that the team is actively examining in order to evaluate the IATAC taxonomy. These values follow industry best practices and serve as the measuring mechanisms for the creation of an intuitive, balanced taxonomy at IATAC. They are listed along with the taxonomy drivers, definitions, and the implications of their use.

Taxonomy Benefits

The benefits that can be realized from a well-defined, intuitive taxonomy are numerous and can be obtained through the phased approach described in this article. These benefits and the value realized by an organization are proportional to a taxonomy's alignment with client objectives and expectations. Unfortunately, many organizations develop taxonomies without first establishing a clear business purpose. Table 3 (see next page) outlines the taxonomy deployment drivers most commonly seen when justifying a taxonomy project and links these drivers to a set of corresponding benefits.

Conclusion

In the case of the IATAC TEMS Project, the goal of the taxonomy project is to convert quantities of vital data from paper format into electronic format and to provide users a convenient way to access and retrieve this data. By following the methodology outlined in this article, the Taxonomy team is developing, testing, modifying and applying the IATAC taxonomy being used to categorize the vast number of documents at IATAC and that is the basis for the web-based GUI that will be used to browse and search for and locate documents. Furthermore, the team is helping to ensure that the IATAC taxonomy provides its intended benefits beyond the immediate scope of the project by providing the steps that, when followed, will allow IATAC to examine and modify the IATAC taxonomy as the number and nature of IATAC documents change over time. ■

About the Author

Gopal Swamy

Mr. Gopal Swamy currently works on strategy, design, and implementation of commercial-off-the-shelf (COTS) Web portal, content management, and knowledge management systems for Intranets, Extranets, and public facing Web sites. He has put his experience to use for a variety of clients in both the civil and defense arenas and may be reached at iatac@dtic.mil. Mr. Swamy holds a Bachelors Degree in Economics from Brandeis University.

Table 2. Taxonomy Validation Values, Definitions and Implications

Taxonomy Driver	Value	Definition	Implications
Taxonomy Breadth	Number of Categories at Highest Taxonomy Level	This defines the total number of categories at the highest level of taxonomy	By ensuring that there are not an excessive number of highest level categories at IATAC, the taxonomy team ensures that IATAC documents have only a reasonable number of categories in which to be placed—thereby making location of documents easier.
	Number of Documents per Category at Highest Taxonomy Level	This compares the number of documents that are categorized into the various categories comprising highest level of taxonomy	By comparing the number of documents in the various categories at the highest level of taxonomy, the taxonomy team ensures the validity of each high level category ensuring the validity of the IATAC taxonomy.
Taxonomy Depth	Number of Subcategories at All Taxonomy Levels	This compares the number of subcategories at each taxonomy level	By evaluating that the number of subcategories at each taxonomy level the taxonomy team ensures that the relationship between the number of subcategories at each taxonomy level is consistent ensuring that documents are not clustered too closely or spread out too broadly making location of documents easier.
	Amount of Content per Category at All Taxonomy Levels	This compares the number of documents that are categorized into the various categories comprising all remaining levels of taxonomy	By comparing the number of documents in the various categories at all taxonomy levels, the taxonomy team ensures the validity of each lower level category ensuring the validity of the IATAC taxonomy.
Taxonomical Distribution	Number of Categories Into Which Documents Are Placed	This shows the total number of categories into which a given document is placed	By capturing the number of times a single document appears in all the categories that comprise the IATAC taxonomy, the taxonomy team can ensure that the document is neither being placed into too many categories, nor too few.

Table 3. Drivers for Taxonomy Development

Drivers	Benefits
Supports Information Retrieval and Discovery	By far the biggest benefit, this driver ties directly into the needs of an organization's staff, customers or web site end-users. Organizing fragmented information leads to more effective information retrieval and to the discovery of important relationships and connections between documents and other pieces of information.
Reduces Duplication of Work	This driver reduces unnecessary document and information creation and categorization while it standardizes and provides consistent access to information across disciplines.
Encourages Increased User Interaction and Organizational Synergy	This driver accelerates the connections between those who are searching for information and those who create information through content triggers and increases community building and collaboration via a controlled vocabulary and a consistent reference framework. This in turn reduces costs and increases innovation—particularly across divisional and geographic boundaries.
Demonstrates External Credibility and Leadership	This driver demonstrates an external credibility and leadership that results from a consistent view into an organization or agency's documentation and information.
Resolves Organizational Issues Regarding Terminology	Through developing taxonomies, this driver ensures consensus regarding the language and meanings of specific terms.

DoD Cyber Crime Center (DC3)

by Steve Shirley

Let's say you're a US Department of Defense (DoD) organization suffering a curious network issue that appears to be more than the common nuisance probe. After your network staff confers with your supporting CERT and the Joint Task Force–Global Network Operations (JTF-GNO), a Cyber Crime Investigator (CCI) from your supporting DoD investigative organization arrives to talk. Let's further say your staff and the CCI agree there's something at work that has penetrated your security measures and may be exfiltrating your data. Bad scenario all the way around.

Before the bad guys tank your network or exfiltrate the crown jewels, who can you turn to help you understand the problem? And, oh, yeah, they've got to be able to mirror-image terabyte-sized slices of data (without tanking your network), handle multiple classification levels and the potential for classified spillage, and do an expert digital forensic analysis to ascertain the problem. They also have to show up in court to explain it, if testifying becomes necessary.

Since late 1998, defense criminal and counterintelligence organizations have been quietly building that capability in the vicinity of Ft Meade, MD: the DoD Cyber Crime Center, or "DC3." These efforts were propelled by the far-reaching vision of Dr. John Hamre, then Deputy Secretary of Defense, when he urged the Air Force Office of Special Investigations, the Naval Criminal Investigative Service, the Army Criminal Investigation Division, the Defense Criminal Investigative Service, and military intelligence to get out in front of the cyber issues proliferating today.

Today, with approximately 200 people, the DC3 comprises three major elements:

1. The Defense Computer Investigations Training Program (DCITP)

2. The Defense Cyber Crime Institute (DCCI)

3. The Defense Computer Forensics Lab (DCFL).

So what does that mean in addressing your problem?

The CCI who arrived to confer with your network staff will have more than likely been one of the 5,000 people trained by the DCITP through its extensive suite of courses on digital forensics and computer crime scenarios. The hardware and software tools used by the CCI and, more exhaustively, by the DCFL, will have been identified or developed by DCCI in its futures exploration role and meticulously tested and validated for function and reliability by the DCCI. But, with its nearly 90 people and 62 "testifying analysts," it's the DCFL who will deliver the digital forensics capability you need to autopsy the digital scene of the crime at the byte-by-byte level.

Even better, the DCFL is one of about a half-dozen digital forensics labs in the US today that is accredited by the American Society of Crime Lab Directors/Lab Accreditation Board (ASCLD/LAB). ASCLD/LAB is the pre-eminent US certifying body for all the crime-labs popularized by TV shows like CSI. But when you consider that the other accredited digital evidence labs range from approximately four to 12 people, according to DCFL director Lt Col Ken Zatyko (USAF), DCFL is by far the largest digital evidence lab.

More significantly, says DC3 Executive Director Steve Shirley reports that it's the only one that exists in a synergistic cyber complex. Plus, as the reliance on cyber capabilities has deepened and broadened with the Global Information Grid (GIG) and NetCentric Operations, Shirley emphasizes that "DC3 is highly oriented at teaming" with DoD organizations with cyber roles and missions. As an example, he cites a recent initiative called the Defense Cyber Ops Group (DCOG) that he chairs for the defense criminal and counterintelligence organizations. It's an initiative to ensure better synchronization, unity of effort, and agility among the DoD CCI's in responding to broad-scoped cyber events that affect DoD. While describing it as a work in progress, "Think of it as a standing posse for the Commander, JTF-GNO, to call on," says Shirley.

continued on page 36…

Quarterbacking Information Management—A Content Staging Overview

by Michael Zizza

A nose tackle and two defensive linemen are slamming into your offensive line. The middle linebacker decides to blitz, and all of your receivers are covered. To make matters worse, it's the fourth quarter, your head coach is screaming on the sideline, the offensive coordinator is yelling through your embedded helmet radio, and your back-up quarterback is sending hand signals. Should you dump the ball off to your fullback, heave it downfield to your tight end in double coverage, or just run? It's not easy being a quarterback in football—deluged with information from different sources, multiple threats, a game plan gone haywire, and much on the line. Now, with infinitely higher stakes, imagine being an Army chief of staff or executive officer in Operation Iraqi Freedom (OIF).

These "quarterbacks" are also overwhelmed with numerous information sources and events that one way or another will support courses of action that commanders must choose. The descriptions of these events and raw intelligence vary in both relevance and quality. For example, the process of supporting "intelligence preparation of the battlefield" means that a staff organization must filter and process information from multiple organizations: the Defense Information Agency (DIA), the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Joint Intelligence Directorate (J2), coalition partners, ground Human Resources Intelligence (HUMINT) on multiple networks; and the Secret Internet Protocol Router Network (SIPRNET), the Non-Classified Internet Protocol Router Network (NIPRNET), the Joint Worldwide Intelligence Communications System (JWICS), the Combined Enterprise Regional Information Exchange System (CENTRIXS), Navy/Marine Corps Intranet (NMCI), and the commercial Internet on multiple platforms. These conditions fuel an often disjointed approach to information management and challenge rather than complement accelerated decision making. Nevertheless, staffs must continue to deliver results to commanders and ultimately accomplish the greater goal of nation building and security in Iraq. Moreover, asymmetric threats, such as roadside Improvised Explosive Devices (IEDs) and guerrilla fighters, combined with extreme pressure for results, yields an accelerated Operating/Operations Tempo (OPTEMPO), which fosters a drastically reduced decision-making cycle and thrusts a chief of staff into a perpetual "two-minute offense."

The current information-management system struggles to keep pace. Knowledge management and business processes must be dynamic and help the process rather than add complexity to an already chaotic environment.

Recognizing this condition as early as 2000, Secretary of Defense Donald H. Rumsfeld and the Department of Defense (DoD) mandated the adoption of "net-centric" information management to deliver speed, efficiency, and ultimately decision-making superiority over a modern enemy.

NetOps is one aggressive initiative that is breaking down old paradigms and embracing assured network and information protection. The idea of Content Staging drives a transformational perspective related to service-oriented architectures. It renovates the aforementioned information streams that currently challenge a chief of staff and his dynamic Communities of Interest (COI). The idea of Content Staging can improve a chief's ability to quarterback a staff and its information-management function and to better support the commander and the wartime mission.

To understand Content Staging, it is helpful to break down its functionality into general tenets or service-like components—distribution, retrieval, cataloging, storage, and safeguarding. (See Figure 1.)

Distribution—This involves tailoring information products for temporary or permanent COIs. Distribution does not mean pushing categories of data to their functional and corresponding users in a top-down fashion. Instead, distribution in the NetOps context means implementing a smart, user-driven philosophy in delivering filtered, high-utility products. Distribution leverages Web-service technologies, such as "messaging," that can facilitate alerts as well as publish and subscribe services to COI-based channels. As a result, leaders can guide information to specific user groups or pull relevant information to support a mission. This promotes logical data dissemination and archiving—efforts that can help stabilize and bring order to the information-management process. For

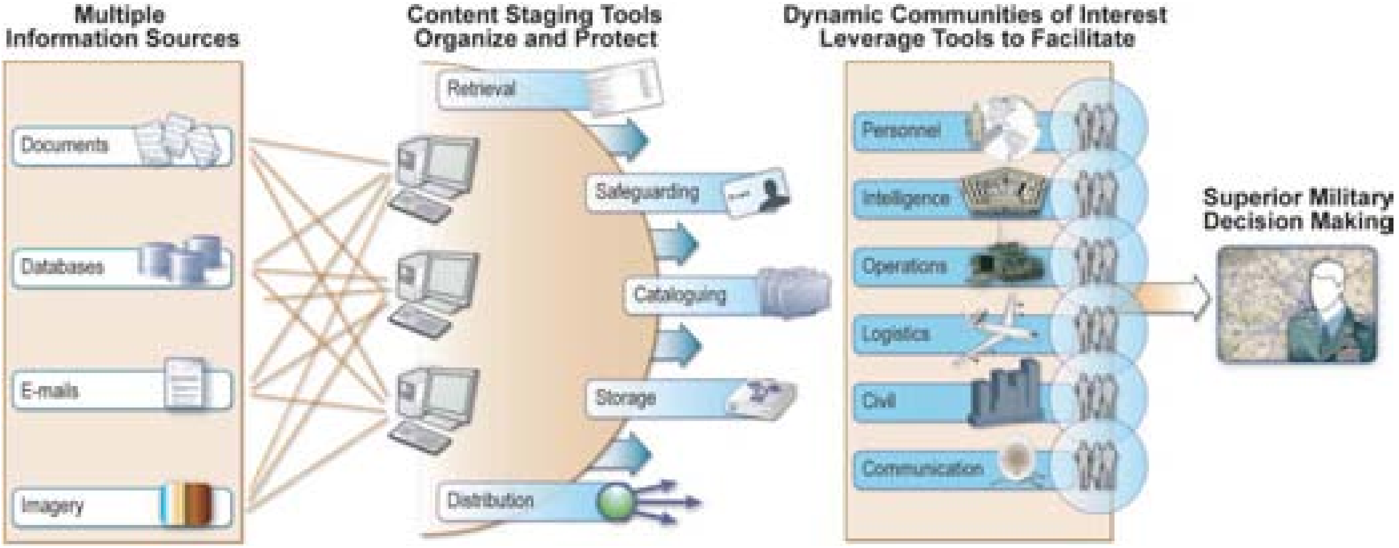

Multiple Information Sources
Documents
Databases
E-mails
Imagery
Content Staging Tools Organize and Protect
Retrieval
Safeguarding
Cataloguing
Storage
Distribution
Dynamic Communities of Interest Leverage Tools to Facilitate
Personnel
Intelligence
Operations
Logistics
Civil
Communication
Superior Military Decision Making

Figure 1. An Overview of Content Staging Categories

example, a cell within an Army or Marine Corps Division component intelligence staff officer (G2) shop would be able to publish and subscribe to a Size, Activity, Location, Unit, Time, and Equipment (SALUTE) report folder from one of its subordinate platoons, Corps G2 Intelligence Summary (INTSUM) folder, and/or relevant intelligence sources within its Operational Availability (AO), such as the DIA or the CIA. The cell's ability to manage information in this way—*via* one domain—would allow it to vet and produce rapid, higher-utility intelligence products to support a commander's current and future battle.

Retrieval—Of course, users cannot anticipate every information requirement. The "fog of war" and unexpected events (Improvised Explosive Device (IED) incidents, insurgent activity) will always result in the ability to retrieve new information for appropriate plans and operations. In the current system, chiefs of staff and their organizations are forced to operate across different portals, workstations, and often networks to collect information and conduct research. Consider the case of legal research. Often an attorney can use a single search tool, such as Lexis Nexus, to explore past cases, the civil and penal code, or court rulings to prepare for a client's proceeding. Conversely, the Army captain in Division G2 must search a local Sharepoint portal for past operations orders, NIPRNET for logistics support data, and possibly a SIPRNET portal for intelligence reports. Web services in the Content Staging realm of Retrieval can facilitate a single search capability *via* Web parts that federate previously separate search results. Therefore, in the previous example, an Army captain, could leverage a single search—much like the attorney—to research and develop intelligence products.

Cataloging—For discoverable content to be fully realized in a net-centric way *via* federated search and other means, users must also be able to catalog exposed information sources. Catalogs are built by appending "metadata" to individual data sources. The ability to add or remove "metadata" promotes the ability to literally stage content for users. Thus cataloged content becomes available to a multitude of users. Perhaps the greatest challenge to Content Staging's concept of cataloging is the old paradigms of "need-to-know" and closely guarded information holdings—a condition that continues to haunt various commands. As mentioned previously, Content Staging and net-centric transformation at large is both a cultural and technological movement. In short, users must embrace both to truly operationalize NetOps. The vision of making sense in information management is certainly hindered if a chief of staff has organic or external organizations limiting catalog creation and not exposing information.

Storage—Content Staging also includes a storage service. The ability to archive and retrieve exposed information is clearly enhanced if there is storage space at both the local and venture levels. Using Web-services technology, Content Staging and NetOps support the establishment of venture-wide storage across different organizations and COIs to augment limited local storage locations.

Safeguarding—Finally, information-management systems at rear and forward locations must be safeguarded across domains and among different users to include coalition, reconstruction, and non-DoD agencies. As mentioned previously, an Army Division staff in OIF must maintain several networks; SIPRNET, NIPRNET, *etc.* to safeguard information across different domains and security levels. Though still under development, Content Staging intends to adopt information assurance advances in cross-domain information exchange (*e.g.*, SIPRNET to JWICS) and discretionary access control (Top Secret to Secret). Any advances in information management that contribute to a user's ability to both safeguard and free information flow will harness these concepts.

The premise of Content Staging as one of NetOps' mission and functional areas supports the spirit of DoD's Net-Centric transformation. With Content Staging, information management can evolve from a stovepiped, disorderly archetype to a federated, joint, and interoperable business process. Taken collectively, the Content Staging services of distribution, retrieval, cataloging, storage, and safeguarding can empower a chief of staff to realize true "economy of force" in information management. The demands of major theater combat operations and modern stability and support operations will likely not decrease in today's war on terror, but information management can increase effectiveness in mitigating the same demands. Technology and cultural change as described by Content Staging's services can assist a chief of staff in effectively quarterbacking his team—through quick and clear decision making—toward victory. ■

About the Author

Mike Zizza

Mr. Mike Zizza has provided systems engineering and management consulting services for several programs, including DISA's Defense Collaboration Tool Suite, the Office of the Secretary of Defense (OSD) Horizontal Fusion, and DISA's Content Staging operational-integration effort. As an Army Ordnance and Field Artillery officer, Mike supported Operations Joint Endeavor and Noble Eagle respectively while serving with III Corps and the 29th Infantry Division. He holds a BS degree in Political and Computer Science from the United States Military Academy at West Point and a Graduate Certificate in Technology Leadership from the University of Virginia. He is currently pursuing an MBA from Indiana University's Kelley School of Business.

…continued from page 33

Providing digital forensics capability to that posse and DoD organizations is where its leadership says DC3 really shines. For example, Lt Col Zatyko indicated that many US state and local digital evidence labs struggle under backlogs and talk in terms of 15–18 months for lab reports to supported agencies. By contrast, says Zatyko, DCFL shoots for a 60-day average and is meeting that target. Preston Thomas, a Naval Criminal Investigations Service special agent, directs DC3's schoolhouse. Our DCITP, says Thomas, "is a superb digital forensics training facility for the DoD." He notes the program has been widely recognized beyond the DoD by other federal investigative agencies that seek seats on a reimbursable basis when a DoD student vacancy occurs.

"What DC3 is really good at is recognizing and adapting Research & Development (R&D) innovations for practical cyber investigative applications," says Special Agent Jim Christy. Christy, who directs DC3''s Defense Cyber Crime Institute, elaborated that DCFL needed a software tool to forensically copy suspect media. "We liked LINUX as a starting point because it was free [and offered] publicly available source code," he said, "but it didn't do key things if you need to prove the mirror-image you've made is identical to the original file." He described that DCCI enhanced LINUX features by adding the capability to copy and verify (algorithm) hash values to allow DCFL examiners to demonstrate that the mirror-image copy subjected to forensic analysis was identical to the unique hash value of the original digital file in evidence. "Solving that practical problem created a tool ("DCCI dd") that has become a standard in forensics examinations."

"DCCI dd" is available to the public through DCCI. For this or other information about DC3's capabilities, you may visit their web site at http://www.dc3.gov or contact Jim Christy at 410/410-1018. ■

About the Author

Steven Shirley

Mr. Steven Shirley is the Executive Director of the Defense Cyber Crime Center (DC3). Mr Shirley is a career AFOSI Special Agent. Spanning 30+ years of Air Force active duty service, to include five tours in Europe and Asia, Mr Shirley led investigative units at every level of the Air Force. He also served as a counterintelligence support officer to a unified command; and was a principal advisor to the Deputy Under Secretary of Defense (Security Policy) in developing positions to protect Department of Defense sensitive programs during arms control treaty inspections. Immediately prior to his DC3 duties, he served as the AFOSI Vice Commander, or chief operating officer, for a worldwide organization with 2,400 people operating at 191 locations around the globe. He is a member of the Senior Executive Service.

We’re moving

IATAC will moving at the end of February.
Our new location will be:
One Dulles Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Our website and email will remain the same:
http://iac.dtic.mil/iatac
iatac@dtic.mil

More information to follow in the next IAnewsletter...

IATAC

IATAC Conference and Event Planning

Experienced Assistance for Your Classified or Unclassified Event

Are you a government client in need of planning and hosting assistance for an upcoming conference? Look no further…

IATAC's conference and event planners provide the assistance you need.

Since 1998, we have offered a full range of services to support classified and unclassified conferences, meetings, and other gatherings for groups ranging from 20 to 300+ participants. From site selection and registration to catering and security requirements coordination, we can plan and execute an event that complies with government conference regulations and provides a high level of customer satisfaction. All members of our staff hold active security clearances ranging from Secret to Top Secret/SCI.

Services are available to all government clients regardless of whether or not they are currently affiliated with the IATAC contract. Support can be arranged through Technical Area Tasks (TATs) subscription accounts with payments *via* Military Interdepartmental Purchase Requests (MIPRs), if applicable.

Our experienced planners offer service and support for all phases of your event.

Before the event

- Site selection
- Budget oversight
- Contract negotiation
- Secure online registration and payment
- Graphics support
- Audio/visual coordination
- Agenda development
- Sponsorship/exhibitor solicitation
- Marketing and promotion
- Security requirements coordination (classified events)

During the event

- Check-in and registration
- Collection of registration fees
- Note-taking (session minutes)
- Speaker assistance
- Problem resolution
- Catering coordination

After the event

- After-action report
- Conference surveys and evaluations
- Distribution of conference proceedings
- Reconciliation of invoices and registration fees

Want more information?

To find out more about IATAC's conference and event planners and what they can do for you, please contact:

April Perera
Director, Conference and Event Planning
703/289-5699

Avery-Lynn Dickey
Conference and Event Planner
703/289-5559

Team e-mail: iatac@dtic.mil

Examples of recent events

Federal PKI Deployment Workshop,
March 2003

Federal PKI Deployment Workshop 2: Federal Credentialing and Beyond,
May 2004

Intel Support to CND Conference,
August 2003

Second Intel Support to CND Conference,
February 2004

Fourth Intel Support to CND Conference,
March 2005

The Political/Military Dimensions of Cyber Security,
March 2004

Treasury IT Security Conference 2004: Making the Grade,
June 2004

DoD Defense Continuity Conference,
September 2004

Joint Task Force for Global Network Operations (JTF-GNO) Component Commanders Conference,
January 2005

JTF–GNO Reporting Working Group,
February 2005

GO/FO/SES Global NetOps Conference,
July 2005

product order form

Instructions: All IATAC **LIMITED DISTRIBUTION** reports are distributed through DTIC. If you are not a registered DTIC user, you must do so **prior** to ordering any IATAC products (unless you are DoD or Government personnel). **To register On-line: http://www.dtic.mil/dtic/registration.**
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name ________________________________ DTIC User Code ____________________

Organization ____________________________ Ofc. Symbol ____________________

Address ________________________________ Phone ____________________

________________________________ E-mail ____________________

________________________________ Fax ____________________

Please check one: □ USA □ USMC □ USN □ USAF □ DoD
□ Industry □ Academia □ Gov't □ Other

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: ____________________

____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

□ Firewalls □ Intrusion Detection □ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics (soft copy only) □ Computer Forensics* (soft copy only) □ Configuration Management
□ Defense in Depth (soft copy only) □ Data Mining (soft copy only)
□ IA Metrics (soft copy only) □ Network Centric Warfare
□ Wireless Wide Area Network (WWAN) Security □ Exploring Biotechnology (soft copy only)

State-of-the-Art Reports (SOARs)

□ Data Embedding for IA (soft copy only) □ IO/IA Visualization Technologies (soft copy only)
□ Modeling & Simulation for IA □ Malicious Code

* You MUST supply your DTIC user code before these reports will be shipped to you.

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

Volumes 4		□ No. 2	□ No. 3	□ No. 4
Volumes 5	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 6	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 7	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 8	□ No. 1	□ No. 2	□ No. 3	

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/IA_newsletter.html

Fax completed form to IATAC at 703/289-5467

December

21st Annual Computer Security Applications Conference

December 5–9, 2005
Marriott University Park, Tucson, AZ
http://www.acsac.org

USSOCOM Conference and Exhibition

December 6–8, 2005
Tampa Convention Center, Tampa, FL
http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_1LP0TIEM0&MID=6630

Security in Storage Workshop

December 13, 2005
Holiday Inn Golden Gate, San Francisco, CA
http://ieeeia.org/sisw/2005/index.htm

Future Ground Forces

December 13–14, 2005
Sheraton Premiere Hotel at Tyson's Corner, Vienna, VA
http://www.idga.org/cgi-bin/templates/genevent.html?topic=329&event=8306&

January

DoD Cyber Crime Conference

January 9–13, 2006
Westin Innisbrook Resort, Palm Harbor, FL
https://www.technologyforums.com/dodcybercrime/index.asp

Network Centric Warfare 2006

January 18–19, 2006
Ronald Reagan Building and International Trade Center, Washington, DC
http://idga.org/cgi-bin/templates/singlecell.html?topic=221&event=8126

TechNet Orlando 2006

January 24–26, 2006
Radisson University Hotel, Orlando, FL
http://www.afcea-orlando.org/documents/TechNet%20Orlando%202006%20v.1.doc

Tactical Power Sources Sumit

January 24–26, 2006
Ronald Reagan Building and International Trade Center, Washington, DC
http://idga.org/cgi-bin/templates/singlecell.html?topic=221&event=8638

Image Fusion 2006

January 31–February 6, 2006
Hilton Washington DC/Silver Spring, Washington, DC
http://idga.org/cgi-bin/templates/singlecell.html?topic=221&event=8626

Phoenix Challenge 2006 Conference–Baltimore

January 31–February 6, 2006
Johns Hopkins University Applied Physics Laboratory, Laurel, MD
http://phoenixchallenge.lackland.af.mil/

February

Homeland Security Conference 2006

February 22–23, 2006
Ronald Reagan International Trade Center
Washington, DC
http://www.afcea.org/events/homeland/

IATAC

Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042

To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at the address above or call us at: 703/289-5454, fax us at: 703/289-5467, or send us a message at: iatac@dtic.mil