○ ISSUE 1 | ○ SPRING | ○ 2006 **The Association for Enterprise Integration**

Enterprise *focus*

INFORMATION SHARING ACROSS EXTENDED ENTERPRISES

Are You Ready for PKI?

In August of 2004 President Bush issued Homeland Security Presidential Directive 12, requiring all Government employees and contractors with access to Federal buildings to have a secure and reliable form of identity. In response, NIST developed FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 14 2006. This standard specifies the X.509 digital certificate in a Public Key Infrastructure.

DoD PKI

The Department of Defense established a program management office for PKI in April, 1999, and has been issuing Common Access Cards with certificates for several years. The early approach was very DoD-centric and only recognized certificates from one root, or PKI. That source was, of course, DoD. But this did not solve the problem of external contractors needing to have credentials. Two External Certificate Authorities (ECAs) were created from which one can purchase, after identity proofing, a certificate. This approach works for DoD on an internal level, but has serious drawbacks for industry - it does not scale easily or efficiently.

Industry Issues

Industry is faced with their own needs for implementing credentialing infrastructures to secure information and sensitive facilities. Companies have been investing heavily in building an internal identity verification capability. Having to buy thousands of additional certificates from an ECA to satisfy a DoD requirement would add significant cost contractors and to DoD programs.

Coalition Problems

Moreover, when put against the policy of warfighting coalitions that has evolved from our Iraq experience, it simply can not work. Coalition partners are sovereign governments and find the notion of having to purchase a DoD-issued certificate to participate in a coalition rather unacceptable. The United Kingdom Ministry of Defence is already dealing with this issue in a very forceful way by participating and funding the Transatlantic Secure Collaboration Programme (TSCP), which is piloting secure collaboration solutions amongst our biggest and brightest defense firms.

Continued on page 3…

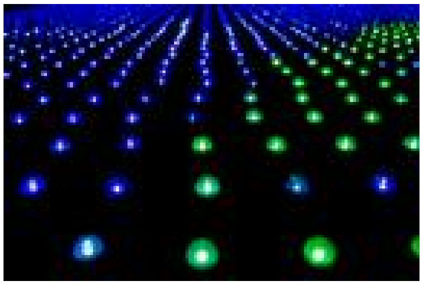
MEETING WATCH

For more information go to www.afei.org

- **April 5 – 6**, Defense Budgets and Programs, McGraw Hill and NDIA, Arlington, VA
- **May 9 – 10**, Warfighters Vision 2006, St. Petersburg FL with General John P. Abizaid, CENTCOM, SOCOM and the Pelican Chapter of AFCEA.
- **May 18**, Trusted Information Sharing, Alexandria, VA with DoD CIO and UK Ministry of Defense
- **June 1 – 2,** Research Directions for Information Sharing, 2010, Washington, D.C. with DoD CIO and DUSD (AS&C)
- **June 27**, Software Assurance and Security Policy Management, Alexandria, VA

Improving Information Assurance

By **STEPHEN F. DEANGELIS** with **DARREL LOWERY**, Enterra Solutions, Inc.



All organizations operate in an environment of extreme complexity and stress. On a daily basis, they face:

- Security and continuity threats, e.g., terrorist attacks, cyber-intrusions, internal/external criminal activity, and natural disasters
- Demands of competition and performance.
- Compliance pressures (e.g., complex regulations, directives, and policies) which create a never-ending series of demands.

Leaders must ensure that organizations meet these demands, fulfill their missions in the face of all threats and risks, and take swift advantage of opportunities. The problem is that events now move at such a rapid pace that reliance on manual processes or responses is both impractical and risky, especially when it comes to Information Assurance. Information Assurance in 2006 has two main components: security and trust. Rule Set Automation™ is the key to systemically addressing these components. Information Assurance responses must leverage automated rule sets to protect enterprise nodes from cyber-attack. For example they must detect intrusions and launch countermeasures faster and more accurately than human network operators could hope to achieve while preserving basic levels of trust between the nodes.

What does "trust between nodes" mean? Yesterday, trust was established inside the walls of the silos of information systems or other systems that existed within a governmental agency, or corporation or business unit. This was the "Monolith". Today, as we try to connect the dots and break down silos within governmental or corporate organizations to move towards the "Matrix" -- the Global Information Grid ("GIG") or Integrated Supply Chains or ("ISC") – we need to establish trust in the silos, or "Nodes," that are going to be members of the GIG or an ISC, so that they are:

- **Secure:** meeting a minimum level of software and information assurance standards and protocols;
- **Compliant:** with the requisite rules and regulations that apply; and
- **Efficient:** with lean and optimized processes and procedures that integrate core shared best practices and, in many cases, performance metrics.

Rule Set Automation is the systemic means of making this happen. Rule Set Automation involves the conversion of rules (in the generic sense, encompassing security rules, compliance regulations, internal controls, performance metrics, contingency plans, tacit knowledge, standard operating procedures and best practices) into automated processes. What this means is documented directives or instructions, usually existing in natural language form (i.e., prose contained in regulations, policies, commander's intent, etc.), are translated into process centric, machine-executable code.

Rule Set Automation gives today's leaders what they most need – systems that provide high visibility, insight, dynamic control and responsiveness. In general – within but also beyond the scope of information assurance – systems ought to provide:

- Real-time information about external events and internal processes.
- The ability to effectively intervene in those events and processes with dynamic rules and inherent information assurance.
- A trusted environment that will efficiently marshal information from any point and direct it to any other point.
- The ability to redirect and adapt resources as needed when a threat arises or an opportunity emerges.

Most systems fall short of this ideal. Over time, most organizations have to deal with greater complexity, geographic reach, and interdependence. At the same time, the world also becomes more complex – global, interconnected and accelerated. Today's information and organizational systems – with their roots in the Monolith -- do not keep pace with information assurance, regulatory compliance and other key factors needed to make the organization resilient. Because of that, federal agency structures address only part of the challenge, not the whole. Government security divisions of agencies and their associated security systems often operate separately from their compliance and performance counterparts. Critical processes are executed in isolation and information assurance is not built into the enterprise. Resources are duplicated, costs increase, and internal friction detracts from organizational responsiveness. Execution is subject to variation – there is inconsistency and human error. Such organizations lack visibility into their own operations – they are, too often, blind to critical events.

Organizations need a fundamentally new approach – one that takes into account current realities, dynamic rules and policy implementation, and takes full advantage of organizational best practices and the most advanced proven technology. And this approach must be standards-based.

Continued on page 4…

> ***Information Assurance in 2006 has two main components: security and trust.***

GAO Critical of DoD Management of GIG

In a of January 2006 GAO report entitled *DoD Management Approach and Processes Not Well-Suited to Support Development of Global Information Grid*, GAO states:

> "Department of Defense (DOD) officials currently estimate that the department will spend approximately $34 billion through 2011 to develop the core network of the Global Information Grid (GIG), a large and complex undertaking intended to provide on-demand and real-time data and information to the warfighter. DOD views the GIG as the cornerstone of information superiority, a key enabler of network-centric warfare, and a pillar of defense transformation. A high degree of coordination and cooperation is needed to make the GIG a reality. In prior work GAO found that enforcing investment decisions across the military services and assuring management attention and oversight of the GIG effort were key management challenges facing DOD."

GAO's major findings are:

1. DOD's management approach for the GIG, in which no one entity is clearly in charge or accountable for results, is not optimized to enforce investment decisions across the department. The DOD Chief Information Officer has lead responsibility for the GIG development effort, but this office has less influence on investment and program decisions than the military services and defense agencies, which determine investment priorities and manage program development efforts.

The department's three major decision-making processes are not structured to support crosscutting, department-wide development efforts such as the GIG.

Continued on page 4…

Are you ready for PKI?

Continued from page 1…

Federation
The design approach of having a centralized certificate source for all who interact with DoD is recognized as an interim step towards a more complete solution. DoD is working to change its policies without compromising on security. The most workable solution at this point seems to be federation, which is being proven out through TSCP.

Cross-certification is a first step. You build your PKI, I build mine, and then we cross-certify so that we can accept each others certificates. Brilliant for two entities, but an n^2 problem of enormous complexity for DoD, MOD and industry.

Enter the Federal Bridge Certification Authority (FBCA), originally created by GSA to cross-certify PKIs inside the Federal government. It now is cross-certifying with non-government PKIs as well.

Commercial Defense Bridge
TSCP and AFEI partnered to sponsor international collaborative identity management working groups, and to support the creation of a commercial bridge for the defense industry. This bridge, known as Certipath, is a joint venture amongst Exostar, ARINC, and SITA (see http://www.certipath.com).

Today we have the outline of the future for personal identity verification. It is PKI-based, auditable identity certification with federation through cross-certifying bridges and robust certificate management. What's left is to fill in the blanks!

Briefing for Industry
Join AFEI, DoD, MOD and senior industry leaders on May 18, 2006 to learn about how the emerging DoD personal identity verification directive, now in coordination, affects your organization. This meeting, **Trusted Information Sharing**, is similar to one held in London on Jan 11, 2006.

At this meeting Mr. John Taylor, Director General Information, Ministry of Defence in the UK and Ms. Priscilla Guthrie, Deputy Chief Information Officer, Department of Defense will address with you their collective approach to establishing trust mechanisms for multi-national defense programs. Their co-speakers will include major defense companies that are already investing corporately in compliant trust mechanisms to protect sensitive information.

Why is this important to you? DoD will soon require personal identity verification within its contracts as part of a wider need for interoperable identity management. This requirement will be for a DoD-recognized PKI certificate to FIPS- 201/OMB Level 4 assurance.

Collaboration Imperative
Without a clear understanding and agreement on how issues of federation, credentialing and trust will be handled across the industry, we run the risk of driving significant cost and interoperability issues into our businesses.

Your company must share more information with more organizations for successful program management, both nationally and internationally. At the same time there are more policies and regulations emerging that govern the security of information exchanges ranging from financial compliance, export controls, medical information and intellectual property rights to national security and counter-terrorism.

Join us on May 18 to help ensure secure collaboration has an affordable solution.

GAO & Industry Group Critical of FIPS 201

GAO Study
GAO issued a report on March 3 (GAO-06-178) that indicated several government agencies would have a difficult time meeting the October 27 deadline for implementing the FIPS 201 standard for personal identity verification set by OMB.

Based on OMB guidance, agencies have until October 27, 2006, to implement the second part of the standard, which requires them to implement interoperable smart-card based ID systems, OMB said. Agencies have begun to take actions to address this part of the standard. For example, Defense and Interior conducted assessments of technological gaps between their existing systems and the infrastructure required by FIPS 201 but had not yet developed specific designs for card systems that meet FIPS 201 interoperability requirements.

GAO also said agencies may not be able to meet implementation deadlines established by OMB, and more importantly, true interoperability among federal government agencies' smart card programs, one of the major goals of FIPS 201, may not be achieved.
See http://www.gao.gov/new.items/d06178.pdf

Contractual Impacts
ITAA commented to GSA on the Interim Rule amending the FAR to address HSPD-12 and FIPS 201, pointing out that this should be deemed a "significant regulatory action" under 5 USC § 801, and commented on the probable impact to contractors of delays in the required background checks of employees by OMB and the FBI. Given the backlog of security clearances today, the imposition of PIV may result in contract delays and disruptions, having a negative impact on both contractors and the government. See http://www.itaa.org/es/headline.cfm?ID=2265

GAO and the GIG

Continued from page 3…

2. While the department has developed a new process for determining requirements, the framework to assess capability needs is still evolving; the new process is not yet identifying shortfalls and gaps in joint military capabilities on a department-wide basis; and requirements-setting continues to be driven by service perspectives.

3. The resource allocation process is structured in terms of individual service programs and outdated mission areas instead of crosscutting capabilities such as net-centricity, and it is not flexible enough to quickly accommodate requirements resulting from lessons learned or from rapidly emerging technologies.

4. Also, the process for managing acquisitions is unsuited to developing a system of interdependent systems such as the GIG, and DOD has struggled to achieve service buy-in on joint-service development programs to address interoperability problems.

5. Finally, the lack of integration among these three processes makes it difficult to ensure that development efforts are affordable and technically feasible.

The full report, GAO-06-211, is available at www.gao.gov or from the AFEI web site.

VADM Szemborski on QDR and Budget Cuts

VADM Stanley Szemborski, Principle Deputy Director, Program and Analysis, OSD spoke on March 14 at the NDIA Systems Engineering Division Network Centric Operations conference in Norfolk, VA. The Admiral spoke about the fiscal health of the nation, budget deficits and the growing expenditure from mandatory spending programs.

Regarding the QDR he outlined the continuation of the move from a two major theater war posture to one of agility and responsiveness to crisis. He postulated that the use of the military for stabilization, security transition and reconstruction will continue. Our military is the only readily deployable, equipped, trained and disciplined force the nation has to deal with crises of all sorts.

Asked about the impact of Katrina on the QDR, he replied that it will likely have a substantial impact. He noted that half of the discretionary spending in the Federal budget is for defense, leaving the audience to draw its own conclusion regarding likely cuts in defense spending.

This was reinforced by looking at the defense budget from the 50's on and seeing that it exhibits behavior not unlike a sine wave. The last two years have seen a decrease from the most recent apex and the trend seems down. Previous peaks were Korea, Vietnam and the Reagan build-up.

Improving Information Assurance

Continued from page 2…

Rules automation is at the heart of Enterprise Resilience Management, a new best-practices methodology and standards-based technology framework developed by Enterra Solutions that integrates security, compliance and performance management.

Enterprise Resilience Management addresses not just information assurance, but the processes that protect the organization's critical assets; it allows private sector companies in critical infrastructure industries and government agencies involved in national security to respond to the challenges of complex regulation, worldwide competition, technology acceleration and a changing security environment.

Continued on page 6…

XBRL: Transforming Global Business

By **J. KELLY BROWN**, EM Software Solutions, Inc.

On October 1, 2005, eXtensible Business Reporting Language, or XBRL[1], became a mandatory reporting format for over 8,000 U.S. banking institutions. All U.S. banks are now required to submit their quarterly Call Reports to the FDIC, Federal Reserve, and Comptroller of the Currency in XBRL. Additionally all changes to the reporting requirements are pushed out by the FDIC, via XBRL, and are automatically incorporated into the reporting applications and subsequent reports. The results: quarterly reports processing is completed in a few days instead of several weeks, error rates have dropped to near zero, and the data is automatically flowed into the Government's legacy systems for further processing and analysis. For more information see: http://www.xbrl.org/Business/Regulators/FFIEC-White-Paper-31Jan06.pdf

In January 2006, the Chairman of the Securities and Exchange Commission (SEC) announced incentives for companies who join a test group for XBRL filings to go along with its voluntary XBRL submission program. The incentives are in the form of expedited reviews of registration statements and annual reports. According to the SEC, XBRL holds the promise of transforming the static, text-only documents that companies file with the SEC into dynamic financial reports that can be quickly and easily accessed and analyzed. Chairman Christopher Cox's recent remarks at the January XBRL conference are available at: http://www.sec.gov/news/speech.shtml .

Active discussions are ongoing with a number of U.S. Government entities to see how XBRL can be used to support regulators, budget offices, contracting officers, and others. The potential of XBRL is not limited to financial reporting—it has tremendous possibilities in other areas such as healthcare, logistics, acquisition, and other information rich environments.

These examples in the United States are complemented by a number of other international efforts including a recent announcement by the UK Government requiring mandatory use of XBRL for corporate tax returns by March 2010. The Dutch Government has mandated tax filings for all businesses by the end of 2006 and forecasts savings of $300M using XBRL. In February 2006, an XBRL system at the Bank of Japan was established for gathering data from financial institutions. It is initially collecting only Balance Sheet data. However, its scope will gradually expand and it currently has some 500 institutions reporting through the system. XBRL is also gaining a significant foothold in a number of Asian stock exchanges for the reporting and analysis of financial information.

What is XBRL?

XBRL, which stands for eXtensible Business Reporting Language is actually an extension of the longer established XML (eXtensible Markup Language) technology. XML is an extremely flexible, text-based mark-up language for describing and storing data and is the parent of HTML (Hyper Text Markup Language) used for web pages. As an extension of XML, XBRL uses tags to identify and organize information. Consider the following data:

CURRENT ASSETS	
Inventory	10,000
Receivables	30,000
Other Assets	50,000
TOTAL	90,000

An XBRL representation of this data would look like this:

```
<abc-gp:Inventories contextRef=”Current_AsOf” unitRef=”US-Dollars”>10000</abc-gp:Inventories>
<abc-gp:Receivables contextRef=”Current_AsOf” unitRef=”US-Dollars”>30000</abc-gp:Receivables>
<abc-gp:OtherAssets contextRef=”Current_AsOf” unitRef=”US-Dollars”>50000</abc-gp:OtherAssets>
<abc-gp:CurrentAssetsTotal contextRef=”Current_AsOf” unitRef=”US-Dollars”>90000</abc-gp:CurrentAssetsTotal >
```

The tagged information describes the type and format of data and the actual content. While a practiced eye can make sense of the information, the intention is that the XBRL is machine processed to provide user-friendly reports, summaries, and analysis. The machine processing uses taxonomies and formatting specifications to provide user-friendly views of the financial information.

The heart of XBRL lies in taxonomies, which are dictionaries that describe the specific tags for data items, e.g., "Other Assets". These taxonomies are developed and managed by a number of organizations and enable the fluid sharing of data across all users. These taxonomies are still evolving, but have actually been entrenched in a number of organizations that are supporting the use of XBRL for business and financial reporting.

XBRL Benefits

The nature of XBRL ensures that financial reporting is standardized across all those who adopt the standards called for by their respective industries or governing organizations. XBRL International, http://www.xbrl.org, a not-for-profit consortium of about 300 companies and agencies, has been leading the way for XBRL adoption. They offer a number of thoughts on the benefits of XBRL including:

- Significant gains via automation by eliminating expensive manual resources that include time-consuming manual comparison of data, assembly of disparately formatted data, and even tedious data re-entry.
- Cost savings, as shared data can be rapidly consumed by those who collect and manage financial data including governments, regulators, stock exchanges, and other financial data consumers.

Continued on page 6…

XBRL: Transforming Global Business

Continued from page 5…

- The ability to create more flexible reporting systems by enabling the representation of current data and meet evolving needs over time

Getting to an XBRL World
Bringing XBRL to the corporate and government world is going to be a significant challenge and opportunity. The challenge for many companies and organizations lies in understanding XBRL and how to integrate into existing legacy systems. Finance and accounting firms are assembling teams of experts who "speak" XBRL, but most will be challenged by the need for integrated tools to move clients into the next generation of fully-compliant XBRL reporting and analysis, see: www.xbrl.org/us.

In the meantime, there are a number of companies who are developing a range of technologies to:

- Convert existing legacy data into XBRL format.
- Present XBRL-encoded financial reports to consumers.
- Provide a range of analytical tools for collating, comparing, and manipulating XBRL information.
- Manage the various needs to transmit, receive, store, integrate, and maintain the anticipated volumes of XBRL data.

The technologies will result in tools ranging from the desktop to corporate servers and even legacy mainframes. XBRL data and technology will become to the finance world what XML has come to mean to the information technology world.

[1] XBRL^{TM} is a trademark of the American Institute of Certified Public Accounts ("AICPA")

Visit EM Software Solutions at www.emsoftwareinc.com

NEXT ISSUE:

AFEI Working Groups

SOA in Defense

IA Policy Management

Report: Warfighter's Vision Conference

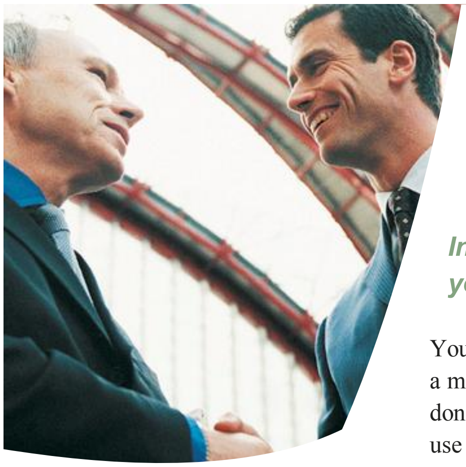
Improving IA

Continued from page 4…

Enterprise Resilience Management identifies an organization's critical assets, the business processes that support those assets, and the rule sets that apply to those processes – and then transforms the rules into executable software code applications and algorithms that run on the organization's IT systems. This approach is grounded in an understanding of core trends that drive the environment, and leverages that understanding as the basis for a new solution built on a trusted enterprise framework.

Enterprise Resilience Management treats the root causes of organizational stress, not just the symptoms, and supports an entire organization, not just discrete functions. As such, it is the answer to most organizations' need for more and better control and the ability to follow through on the rules mandated by eGov, FISMA, Homeland Security Presidential Directives (HSPDs) and other enterprise compliance regulations.

Visit Enterra at www.enterrasolutions.com



You invest your marketing dollars carefully. When you invest them in AFEI two things happen: you are recognized as a serious player in enterprise integration, transformation and net-centricity; and you enable AFEI to continue to build the relationships and programs that benefit its members. Make AFEI one of your first choices for presence, exposure and communications.

Getting the most from membership

Investing in AFEI can be an important part of your strategic communications and marketing

Your membership in AFEI is like a membership in a gym. You don't get any benefis unless you use it! AFEI members have many unique opportunities for interaction with government, industry executives and decision makers at all levels.

AFEI is constantly building new relationships with government agencies and industry leaders - people you want to connect with!

Through these relationships members are able to interact with their customers to build depth and relational credibility.

The ability to get your thought leadership exposed to a wider community is a key member benefit. Through exposure on our AFEI web site, blog, webinars, seminars and conferences your message gets through!

The Association for Enterprise Integration is a subsidiary of the National Defense Industrial Association whose motto is ***"Strength through Industry & Technology"***

GET CONNECTED: Exposure & Involvement

AFEI is rapidly becoming the "go to" association for industry, government, consortia and other associations to collaborate on the difficult issues that surround net-centricity. Our ability to leverage innovation in the commercial sector is one reason leaders gravitate to involvement with AFEI.