

TECHNICAL DOCUMENT 3215
June 2006

Software Support Activity Information Technology Update Newsletter

Third Quarter, FY 2006

Approved for public release;
distribution is unlimited.



SSC San Diego
San Diego, CA 92152-5001

SSC SAN DIEGO
San Diego, California 92152-5001

F. D. Unetic, CAPT, USN
Commanding Officer

C. A. Keeney
Executive Director

ADMINISTRATIVE INFORMATION

This periodical provides a collection of articles written by the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Software Support Activity (SSA) as a consistent method of communicating SSA efforts and vision, while providing awareness of key enterprise challenges. The JPEO-CBD is managed by the Space and Naval Warfare Systems Center San Diego (SSC San Diego) and is directed by the Space and Naval Warfare Systems Command. The SSA is a team composed of government and contractor agencies that provide enterprise support in the key tenets of net-centric operations to U.S. Department of Defense chemical and biological programs.

Released by
D. R. Hardy, Head
Effects Based Information Systems

Under authority of
T. Tiernan, Head
Command and Control
Technology and
Experimentation Division

This is a work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction. Many SSC San Diego public release documents are available in electronic format at <http://www.spawar.navy.mil/sti/publications/pubs/index.html>

Inaugural Issue

JPEO-CBD
SOFTWARE
SUPPORT
ACTIVITY



SSA Information Technology Update

Volume I, Issue I

Q3 FY06

Inside this issue:

Introducing the SSA	1
Terrorist Threats Against Information Systems	4
Integration & Test	4
Architecture	5
Q&A	5
Data Management	6
Science & Technology	6
Standards & Policy	7
Help Desk	7
SSA Highlights	7
Configuration Management	8
Key C&A Concepts	9
The SSA Team	12

Welcome!

Welcome to the inaugural issue of SSA Information Technology Update. The purpose of this newsletter is to highlight the activities and services of the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Software Support Activity (SSA), with the hope that this will educate the reader and help us to better serve you. Ultimately our mission is to increase the survivability of warfighters after Chemical, Biological, Radiological, and Nuclear (CBRN) attacks by promoting the interoperability and integration of CBRN defense systems. We hope this newsletter will help stimulate the conversations and partnering that will result in the successful outcome of this mission.

If you have comments or suggestions on how this newsletter could be more useful to you, please contact Doug Hardy (619•553•5410 or douglas.hardy@navy.mil) or Dick Brimson (619•553•0806 or rbrimson@spawar.navy.mil).

Douglas R. Hardy
SSA Project Manager



By Doug Hardy, JPEO-CBD SSA Manager

Previously published in the Chem-Bio Defense Quarterly magazine, Jan-Mar 2006 issue

Officially chartered by Brig. Gen. Stephen Reeves, Joint Program Executive Officer for Chemical and Biological Defense (JPEO-CBD), on May 31, 2005, the Software Support Activity (SSA) is a user software support activity that spans and supports all JPEO-CBD Joint Program Managers (JPMs) and Directorates. The SSA vision is to be a comprehensive and cost-effective single point of contact for users (customers, developers and warfighters) to receive professional and timely assistance with all Information Technology (IT) related to Chemical, Biological, Radiological, and Nuclear (CBRN) Defense program standards, interoperability, and supportability needs. Ultimately, this vision would result in the creation of more efficient, common, and consistently superior interoperable and integrated CBRN systems for the warfighter.

The SSA is focused on IT programs and systems that transmit, receive, or store CBRN data and how those systems interoperate on networks. For the JPEO-CBD, the SSA brings into focus a sometimes blurred picture of new and emerging standards and policies from a variety of sources; including directives and instructions, that drive architectures, data management, and information assurance; such as, the Department of Defense (DoD) Architecture Framework (DoDAF) products, DoD Net-Centric Operations and Warfare Reference Model, and DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The SSA also works with a variety of JPEO related organi-

(Continued on page 2)



Introducing the Software Support Activity (SSA)

(Continued from page 1)
zations to assist JPMs in clarifying and further understanding requirements, providing insight into potential programs for science and technology transition and insertion, and better understanding of integration and test operations, especially in relation to modeling and simulation (M&S) and verification, validation, and accreditation (VV&A) activities. The SSA vision of bringing into focus the IT environment for all JPEO-CBD JPMs and providing key performance capabilities for CBRN warfighters is reflected in Figure 1.

To provide this assistance, the SSA is forming teams with expertise in several functional areas. Current efforts are concentrated on Architecture, Data Management, Information Assurance, Integration and Test (including Modeling and Simulation), Science and Technology, Standards and Policy, and Customer Support (Help Desk).

ARCHITECTURE

The Architecture team's primary focus is toward implementation of a standard DoDAF compliant Integrated Architecture in JPEO-CBD products. In July 2005, Brig. Gen. Reeves and Maj. Gen. Howard Bromberg (JROCBRND) signed a Memorandum of Understanding (MOU) entitled "Stewardship of Department of Defense (DoD) Chemical, Biological, Radiological, and Nuclear (CBRN) Architecture Products." The purpose of the MOU is "to ensure that the components of the CBRN architecture are developed in a coordinated manner that will result in a fully integrated common CBRN data model and architecture for the CBRN Community of Interest (COI)." After the MOU was signed and in cooperation with the Joint Requirements Office (JRO) Shape Action Officer,

the Architecture team formed a Joint CBRN Architecture Working Group that meets monthly (2nd Wednesday) and includes membership from all JPMs to discuss the various architectural issues and concerns among the programs.

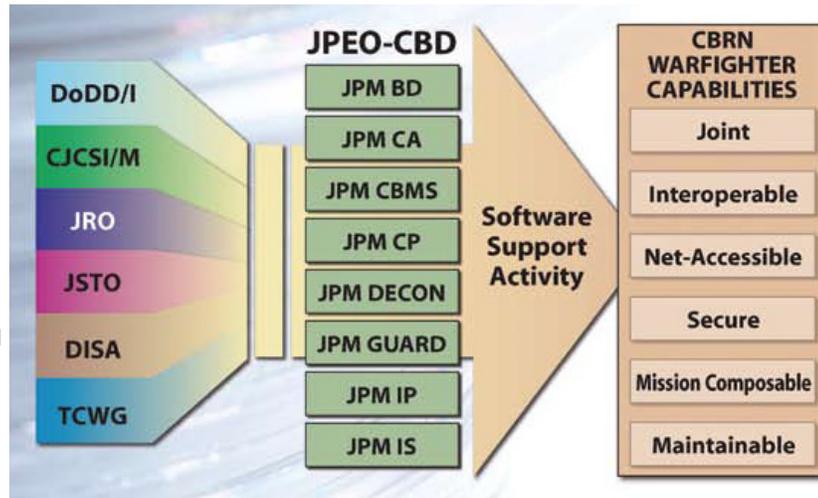


Figure 1. SSA Vision

As a result, Architecture products are being collected and posted to the JPEO-CBD Integrated Digital Environment (IDE) web site (jpeocbd.altess.army.mil). All programs with DoDAF products or interest in DoDAF products or comments/feedback are encouraged to visit the site. Please contact the SSA CM Coordinator, Denise Milligan, at dmilli@spawar.navy.mil, 619-767-4191, or the SSA Architecture Lead, Dave Godso, at godso@spawar.navy.mil, 703-365-9662.

DATA MANAGEMENT

The Data Management team works closely with the architecture team in an effort to cultivate an enterprise-wide data management strategy that promotes interoperability and integration between programs thru the implementation of a common CBRN Data Model.

The CBRN Data Model is registered with the DoD Extensible Markup Language (XML) Metadata Registry as the official Data Model for the CBRN COI Namespace. The Data Management team is actively involved in pursuing and understanding data interface and exchange requirements from a variety of COIs and

the COI Forum. The Data Management Team will be hosting the Data Model Working Group (DMWG) Technical Review for version 1.3 of the CBRN Data Model from 10-12 January 2006 at the Edgewood Chemical Biological Center (ECBC), Aberdeen Proving Ground, Edgewood, MD. The DMWG will provide a broad forum to discuss the latest changes, the future changes for the next release, and recommend other changes and/or improvements to the Data Model. The DMWG has steadily grown, and the last DMWG in July 2005 included 80 attendees. It's not too soon to get your visit requests on file with the Security office. For information concern-

ing this event, contact Bill Snee at wsnee@msiac.dmsi.mil or John MacCrossen at macroscen@spawar.navy.mil.

All programs are encouraged to visit the IDE to see the latest Data Model, including instructions on change requests to the Data Model, which can be made by downloading the form found on the IDE, or by contacting the SSA CM Coordinator. For questions regarding the CBRN Data Model, please contact the CBRN COI Namespace Manager, Dr. Tom Johnson, 831-656-3190 and/or the Deputy Namespace Manager, Bill Snee.

INFORMATION ASSURANCE (IA)

The IA team is providing direct support to several JPMs, with a dozen DITSCAP System Security Authorization Agreements (SSAAs) underway in various stages of completion. The IA team is actively involved in certification and accreditation, and in reviewing new and emerging IA requirements and policies (e.g., DOD Information Assurance Certification and Accreditation Program (DIACAP)) to determine impact to the IT programs and systems. For more information on IA, contact the SSA IA

(Continued on page 3)

Introducing the Software Support Activity (SSA)

(Continued from page 2)
Lead, Guy Casciola, at casciola@spawar.navy.mil.

CUSTOMER SUPPORT (Help Desk)

The Customer Support team has been working to establish the necessary MOUs and business rules to support an initial Level I Chemical and Biological Defense (CBD) IT Help Desk capability. This effort has been aimed at two near-term requirements to support JPM IS programs, Joint Warning and Reporting Network (JWARN) and Joint Effects Model (JEM) milestones. On 15 October, the SSA stood up this Level I CBD IT Help Desk, which provides a Level I Customer Support capability and is now taking calls. The plan is to evolve the MOUs and business rules, and promote this Level I capability as the CBD IT Help Desk that will provide 24/7 support to any number of IT programs once it is fully operational. For more information on the Help Desk, contact the SSA Help Desk Lead, Pat Lowe, at plowe@spawar.navy.mil.

INTEGRATION AND TEST (I&T)

The I&T team is working to develop consistent processes and guidance for program and model accreditation, data certification, and Independent Verification and Validation (IV&V) efforts and looking for opportunities for co-use of the assets and results associated with the many ongoing program test activities. In June 2005, an M&S VV&A Guidelines document generated by the I&T team was signed by the JPEO-CBD. The I&T team is also involved in evaluating M&S strategies for various programs (e.g., JPM

Individual Protective Equipment (IPE)) and in the concept of establishing a JPEO-CBD M&S Center of Excellence. For more information regarding these efforts, contact the SSA I&T Lead, Jennifer Park, at jennifer.park@navy.mil.

SCIENCE AND TECHNOLOGY (S&T)

The S&T representative has recently joined the SSA team to study "transition-able" products with potential to join the already formidable array of technologies in use by the CBRN Defense programs and systems. These include such proposals as a CBRN Medical Pilot proposal that looks at future interoperability between the CBRN and Medical COIs and a Sensor-on-a-Chip Pilot to look at interoperability moved to smaller, in-the-field devices to provide the next generation capability. In coordination with Joint Science and Technology Office (JSTO)/ Defense Threat Reduction Agency (DTRA), these are just two of several pilots and proposed pilots for evaluation and potential insertion into programs. For more information regarding these efforts, contact the SSA S&T Lead, LorRaine Duffy, at lorraine.duffy@navy.mil.

STANDARDS AND POLICY (S&P)

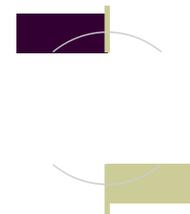
The S&P representative is working to support all of the other areas in understanding and clarifying DoD standards, directives, instructions, and policies. This includes staying abreast of the Army Strategic Software Improvement Program to alert all other areas of opportunities for training and improving processes for acquiring and architecting software sys-

tems. A similar initiative is underway to better understand System Engineering plans and processes that may affect the JPEO-CBD. For more information regarding these efforts, contact the SSA S&P Lead, Dan Reuben.

Shortly after being chartered, the SSA began a series of "Roadshows" to introduce itself to the JPEO-CBD community. The initial round of roadshows concluded in October 2005 and included visits to all JPM and JRO activities. The SSA plans to conduct 2006 follow-on visits based on the information obtained during the initial roadshows.

As the SSA moves forward in 2006, it will pursue objectives that align JPEO-CBD IT products with common architectures and data representation, methodologies that promote interoperability and integration for programs and systems across the enterprise, and further support sustainability and maintenance for the product lifecycle. It will also promote technology insertion and/or re-use from the civilian sector and other communities for mutual benefit of the users and customers of JPEO-CBD products. The SSA seeks to leverage the benefit of pre-existing solutions wherever possible, including standardized language/syntax, data, information assurance, integrated architectures, modeling and simulation, and testing.

"SSA products will provide the tools and information the JPMs need to build toward standardized Information Technology (IT) products with a common JPEO-CBD look and feel, and consistent functionality and interoperability between JPEO-CBD systems"
JPEO-CBD SSA Charter



Information Assurance



By Guy Casciola, JPEO-CBD SSA Information Assurance Lead

Previously published in the Chem-Bio Defense Quarterly magazine, Jan-Mar 2006 issue



Spotlight on Security

The threat of Chemical, Biological, Radiological and Nuclear (CBRN) by terrorists or rebellious entities is increasing each day. The U.S. Government has undertaken several efforts to minimize these attacks by developing Information Technology (IT) systems/networks that can predict where the fallout is and take the appropriate action to protect warfighter's lives. But wait!!!! These IT systems/networks are meant to protect the warfighters, but how do you protect the systems/networks from the terrorists? The answer is easy, by applying Information Assurance (IA) techniques to all of your systems/networks following Department of Defense directives/regulations/instructions.

Let's face it, IA is the proverbial thorn in the side. Many still resist IA to one degree or another, despite the IA programs and mandates already established. Some people believe the process is an overkill or isn't necessary at all. Others believe it's just a drill that generates a lot of paperwork that sits on a shelf and collects dust. In some respects, and in some cases, the critics are right; the process could be viewed overkill. But is it necessary? Absolutely!!! Waiting until an incident occurs before taking action is too late and too costly, because lives are at risk. Anyone who takes the time and effort to create all the necessary documentation without acting on the problems identified, is wasting time and is defeating the purpose.

So why do we need all this security? The Certification and Accreditation (C&A) process is needed to ensure that each and every Information System is being protected against the four impact areas; denial of service, unauthorized disclosure, modification, or destruction. What is needed to protect the IT system/networks against these impact areas is the proper implementation of security safeguards in each system/network and the surrounding environment in which the system/network resides. What comes out of the C&A process is what is known as the System Security Authorization Agreement (SSAA) currently based on the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). If the SSAA documentation proves that the Information System is fully protected, no matter what impact area might occur, the requirement should be satisfied. The following is a brief explanation of these impact areas:

(Continued on page 8)

Integration & Test

The SSA Integration and Test (I&T) Team has been chartered to:

- Coordinate developmental and operational test schedules and activities of JPEO-CBD Information Technology (IT)/ National Security Systems (NSS) across JPMs to minimize expenditures within the enterprise and maximize the opportunities for co-use of facilities,

personnel, and test opportunities.

- Ensure I&T personnel have an adequate understanding of Army, Navy, Air Force and Marine Corps Command, Control, Communications, Computers and Intelligence (C4I) systems and their individual Operational Test Agency (OTA) requirements.

- Provide consistent processes and guidance to JPEO-CBD programs for conducting program and model accreditation, data certification, and Independent Verification and Validation (IV&V).

The I&T group is currently focusing on several initiatives:

(Continued on page 6)



~ I&T ~
The Validation
Of Interoperability

Architecture

The Department of Defense (DoD) defines "Architecture" as "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." As DoD drives all capabilities toward Net-Centric Operations and Warfare (NCOW), architectures provide a critical mechanism for:

- Understanding operational concepts and their relationship to capabilities, technologies, systems, and standards (Figure 1).
- Anticipating changes in operational concepts or changes in automated capabilities.
- Acquiring both materiel and non-materiel assets.
- Developing a roadmap that takes us from where we are to where we want to be.

The SSA Architecture Team looks across the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Programs of Record for common systems and soft-

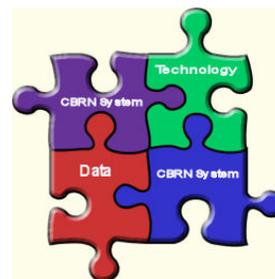
ware engineering themes. The overarching goal is to facilitate reuse and align programs to net-centric Service Oriented Architectures and implementations based on the DoD's Data Strategy. The SSA Architecture Team serves as the JPEO-CBD Software Integrated Product Team (IPT), reporting directly to the JPEO-CBD Chief Systems Engineer (CSE), having Chief Software Architect (CSA) responsibilities across JPEO-CBD.

The JPEO-CBD SSA Architecture Team is chartered to:

1. Develop, validate, and implement a technical Command, Control, Communications, Computers, and Intelligence (C4I) architecture in support of the operational requirement developed by the Joint Requirements Office (JRO) DoD Architecture Framework (DoDAF) compliant Integrated Architecture.
2. Maintain and shape the Integrated Architecture

to address new technology, changing assumptions, and emerging requirements, including transition and mapping to the Global Information Grid (GIG) 2.0 and the NCOW Reference Model (RM).

3. Maintain common frameworks that support and specify integrated individual, fam-



~ Architecture ~
The Structure
Of
Interoperability

ily or system of systems, including applicable operating systems, programming languages, tools, and core components as applicable.

The SSA Architecture Team has three fundamen-

tal operating principles:

1. Provide support to programs requiring expertise in systems and software engineering as it relates to meeting program milestones.
2. Provide strategic technical expertise in terms of specification development, technology evaluation, and identification of common services and standards such that all "information technology" across the Chemical Biological Defense Program (CBDP) can be reused so CBDP programs can focus resources on CBDP-specific problems.
3. Understand the pieces that currently exist, how they relate, where we need to go to achieve the net-centric vision, and provide recommendations to senior leadership to move the Enterprise in DoD's intended "DoD as a net-centric enterprise" direction.

Q&A

Q: What's a WSDL ("wiz dahl")?

A: WSDL stands for Web Services Definition Language and is one way for you to make your information service available on the GIG. It specifies what your service does, where it's located, who the service provider is, what parameters it requires, among other types of information necessary to connect to and use the service. If you have a service, application, or systems which must connect to the GIG, then you probably need to know more about WSDLs, and web service end-points in general. For more information please contact the SSA Architecture team (godso@spawar.navy.mil).



Data Management

The mission of the Joint Project Manager for Information Systems (JPM IS) is to provide the information architecture and applications for shaping the battle space against the chemical and biological threat. The key to those architectures and applications begins and ends with data. The JPM IS has several ongoing events that advance systems interoperability with respect to data. On October 27th, 2005 the JPM IS Data Acquisition Program Manager and the Software Support

Activity (SSA) Data Management Lead presented the "CBRN Data Model Implementation Approach" at the Chemical-Biological Information Systems (CBIS) Conference in Albuquerque, New Mexico. William Snee, the SSA Data Management Lead presented insights into how the CBRN Data Model can be implemented and how it will fit within the CBRN Community of Interest (COI) and a Service Oriented Architecture (SOA). Also presented at the confer-

ence was the "Coordinating CB Engagement Scenarios with the CBRN Data Model" paper. Stephen Helmreich of the University of New Mexico discussed variables and values used in creating chemical and biological engagement scenarios and the correlation between these variables and values with the entities, properties, and values of CBRN Data Model 1.2. The CBIS Conference was an excellent opportunity to discuss, present and

(Continued on page 11)



~ Data ~
The Glue
Of Interoperability

Integration and Test

(Continued from page 4)

- Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A). We are providing expertise to assist the Joint Effects Model (JEM), Joint Operational Effects Federation (JOEF), and Joint Warning and Reporting Network (JWARN) Programs of Record (PoRs) in the preparation of their M&S VV&A plans. Previously we developed the JPEO-CBD M&S VV&A Guidelines for use across all the PoRs within JPEO-CBD.
- In response to a request by Brigadier General Reeves, we have developed a proposal for a M&S Center of Excellence that would be facilitated by personnel from several of our SSA Teams.
- JPM Individual Protection (JPM IP) has requested our help in developing their M&S Strategy and we have brought some new faces on board to assist in that effort..
- A CBRN-Medical Information Sharing Pilot Project has been proposed both within the CBRN and Medical communities and the I&T group is deeply involved in moving that effort forward.

With many new efforts being considered and the stated vision of building an Enterprise-wide net-centric Architecture, the I&T group continues to help identify common solutions and complimentary processes across many domains

For more information, please contact Jennifer Park at jennifer.park@navy.mil.

Science & Technology

The Science and Technology (S&T) Service Center has been given the mandate to provide a centralized clearinghouse for initiating, analyzing, managing, and implementing various innovative efforts from the scientific and technology development arenas into the JPEO-CBD Program. The objective is to immediately harness the potential of next generation technologies, by impressing upon the S&T community, the need for interoperabil-

ity of systems, robustness of architecture, and standardization of data elements for reuse and longevity. The area has several initiatives it is reviewing, focusing on Technology Transition Agreements (TTAs), in order to ensure rapid transition from innovation to standardized component within the DoDAF compliant Integrated Architecture for JPEO-CBD systems. An overarching S&T strategy is being formulated to manage the proposals that the

JPEO-CBD Program receives (currently 20), to focus efforts on technology development and adoption at the appropriate milestone.

Two new initiatives that are of immediate interest include data sharing with the medical communities of interest (COIs) and the concept of net-ready sensors. The first is an effort that would result in a logical data model, XML (eXtensible

(Continued on page 11)



~ S&T ~
The Future
Of Interoperability

Standards & Policy



The SSA Standards and Policy Team supports JPMs and JPEO-CBD in complying with interoperability and supportability requirements mandated for all CBRN defense IT systems and products by the Department of Defense (DoD) and Chairman of the Joint Chiefs of Staff (CJCS).

Support includes collaboration among projects, CJCS, the

Office of the Secretary of Defense (OSD), and the Services to resolve issues, streamline processes, provide reusable templates and artifacts, and leverage assets to help maintain and support JPEO-CBD's most effective use of resources.

JPMs dealing with Joint Capabilities Integration and Development System (JCIDS) compliance can rely on SSA

Policy and Standards to support them in developing compliance documents (such as Information Support Plans (ISP) and advocate with CJCS and OSD to remove impediments and pave the way for projects to comply with mandates for Jointness, certifications, and extensive DoD-wide coordination processes.

(Continued on page 10)

Help Desk

On 15 October 2005, the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Chemical and Biological Defense (CBD) Information Technology (IT) Help Desk came online. The CBD IT Help Desk will provide Level I support to Warfighters using any of the JPEO-CBD IT Products.

Level I: The Help Desk will

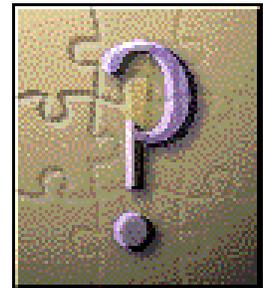
obtain all the needed information from the customer calling, in the form of a Customer Service Request (CSR). They will then pass the ticket/user over to the designated Level II Help Desk or to a Level III Subject Matter Expert (SME), when appropriate.

Initially, during its standup phase, the CBD IT Help Desk will support three JPM IS pro-

grams; JWARN, JEM, and JWARN Initial Capability (JIC). This support will be Level I.

Level II: The Help Desk at this Level will troubleshoot and work with the customers to resolve the CSR. The Help Desk will access the knowledge base, prior experience, and computers running the software to resolve the issues. If

(Continued on page 10)



SSA Highlights

August 2004 - SSA established

February 12, 2005 - CBRN Data Model v1.2 released

May 31, 2005 - Brigadier General Reeves signs the Charter officially standing up the JPEO-CBD SSA

July 13, 2005 - First JCBRND Architecture Working Group (AWG) meeting held

July 15, 2005 - SSA Road Show for JWARN



July 18-21, 2005 - SSA Road Show for JPMs BD, CA, and CBMS

August 31, 2005 - SSA Road Show for JRO Sustain and JPM CP

September 1, 2005 - SSA Road Show for JPMs IPE and Decon

October 6, 2005 - SSA Road Show for JEM

October 7, 2005 - MOU signed with System Support Knowledge Center (SSKC) for Help Desk support

October 15, 2005 - Help Desk goes online

October 24, 2005 - Data Model v1.3 released

“The SSA will provide services and coordination for IT products developed by the JPMs which contain data, software, or which are capable of, or have a requirement for future linkage to the Global Information Grid (GIG).”

JPEO-CBD SSA Charter

Configuration Management

The SSA Configuration Management Team is currently assisting in the implementation of the Memorandum of Understanding (MOU) between the Joint Requirements Office-Chemical, Biological, Radiological, and Nuclear Defense (JRO-CBRND) and the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) for the

stewardship of Department of Defense (DoD) Chemical, Biological, Radiological, and Nuclear (CBRN) architecture and data products.

Two of the key requirements of the MOU are to produce a Joint CBRND (JCBRND) Configuration Management Plan (CMP) and to establish a repository for Joint architecture

and data products on the JPEO-CBD Integrated Digital Environment (IDE) website.

It is anticipated that the JCBRND CMP will be approved late-2nd Quarter or 3rd Quarter FY 2006. The CM Team is in the process of developing the JPEO-CBD IDE repository structure and a

(Continued on page 11)



Terrorist Threats Against Information Systems

(Continued from page 4)

- When the system/network is vulnerable to attacks, the entire system/network could be brought down, thereby, rendering the system/network unavailable so if an attack were to occur, the system/network would not be available to function. This could result in the death of many warfighters. This is known as denial of service in which action or actions that result in the inability of a system/network or any essential part to perform its designated mission, either by loss or degradation of operational capability.
- When the system/network is not properly secured, this could enable

unauthorized individuals, (either by accidental or intentional means), the ability to access the information, thereby, allowing sensitive information to be compromised. Therefore, unauthorized disclo-

sure occurs when exposure of information to individuals not authorized to receive the information, takes place.

tion improperly, which also endangers the warfighters lives. This is considered modification that exists when software/information is altered by changing or adding to its representation, (integrity

is rendered questionable).

- When an attack totally destroys the system/network, then there is no system/network to warn warfighters of possible CBRN attacks. This of course is destruction that exists when any asset is declared 100% economically non-repairable or non-recoverable.

Each Joint Project Manager (JPM) has unique IA problems such as; classification levels, wireless connections, cross-domain situations, etc. Because of the uniqueness, not every situation is covered in an instruction. Some might take the stance that, if their specific

(Continued on page 9)



The SSA Information Assurance Team. Right to left: Guy Casciola (Team Lead), John Howard, Blake Lompfrey, Catrina Brott, Colin Fera. Not pictured: Pat Guerin, Cale Dansbee, Chris Beckham.



~ Information Assurance ~
Safeguarding Systems
Safeguarding Warfighters

“Anyone who takes the time and effort to create all the necessary documentation without acting on the problems identified, is wasting time and is defeating the purpose.”

Terrorist Threats Against Information Systems

(Continued from page 8)

situation requires some type of security measure not covered in an instruction, they don't have to document it. This is not the case. Where instructions are lacking for guidance, best practices should be implemented. In other words, if you really believe some security protection should be employed, then it probably should be. It is better to be safe than sorry. It is up to all JPMs to ensure that the integrity for all Information Systems is maintained, and whatever it takes to accomplish this should be completed. All systems must go through the C&A process before being accredited and deployed for operational use. If not, then per DoD mandates, these systems/networks are in violation and vulnerable to exploitation. Because environments and equipment are always changing, review of the threats and safeguards is an ongoing effort. Remember, going through the C&A process the first time is much harder than maintaining it. The process should be reviewed for re-accreditation at least every three years or when major changes to a system or environment have occurred such as:

- Addition or replacement

of a major component or a significant part of a major system.

- A change in classification level of information processed.
- A significant change to the operating system or executive software.
- A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation.
- A significant change to the physical environment where the system resides.
- A significant change to the threats.
- A significant change to the availability of safeguards.
- A significant change to the user population.
- The passage of three years since the effective date of the existing accreditation.

So, what can you do to accomplish all these regulations? About a year ago the Joint Program Executive Officer for Chemical & Biological Defense (JPEO-CBD) Software Support Activity (SSA) IA team was established to assist all the JPMs by providing C&A support. This team of specialized personnel can ensure your systems/networks are appropriately locked down in order to eliminate or minimize the impact of threats that can cause denial of

service, unauthorized disclosure, modification, or destruction to information system resources.

The SSA IA team members provide a resource of technical expertise in satisfying the requirements of the current DoD IA regulations. Our experience with CBRN unique operating environments and security requirements enables us to help you achieve the DoD mandate of operating each Information System at an acceptable level of risk through the C&A process. Our IA team members have a proven record and reputation of performing each step of the current C&A process leading to accreditation of your Information System. So, you need not look any further than the SSA IA team to provide quality and professional IA services.

For information regarding these SSA IA services, please contact the JPM-IS/SSA Security Manager, Guy Casciola, at casciola@spawar.navy.mil.



SSA IA can assist you through the Certification and Accreditation process

“The SSA IA team has a proven record and reputation of accomplishing each step of the C&A process, leading to the accreditation of your Information System. “

Key C&A Concepts

ATO - Authority To Operate - The formal declaration by the DAA that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards. This is the end goal of the C&A process.

CA- Certification Authority - Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing risks associated with the operating system, coordinating the certification activities, and consolidating the final certification and accreditation package.

DAA - Designated Approval Authority - Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.

DITSCAP - DoD Information Technology Security Certification and Accreditation Process - "The DITSCAP ... defines a process that standardizes all activities leading to a successful accreditation. ... Standardizing the process will minimize risks associated with nonstandard security implementations across shared infrastructure and end systems." (DoD Instruction 5200.40)

IATO - Interim Authority To Operate - Temporary approval granted by a DAA for an Information System to process information based on preliminary results of a security evaluation of the system.

Help Desk

(Continued from page 7)

the issues can not be resolved at this level then the ticket will be referred to a Level III SME.

The future goal of the CBD IT Help Desk is to provide Level I support for all JPEO-CBD Programs of Record. Level II support will be available for any JPEO-CBD Program of Record as a Service-For-Fee.

If Warfighters are having trouble understanding a program feature or simply have a question, they can contact the Help Desk 24/7, by email, telephone, or online. Experts are there to help resolve issues and, if unable to resolve the issue, put the Warfighter in touch with additional resources.

This Help Desk's web site contains links to:

- JPEO-CBD IT Support Website (herein referred to as Help Desk web page)
- request a user account for access to the Help Desk web page
- submit or check the status of a Customer Service Request (CSR)

The Help Desk web page provides Warfighters access to a wide range of program information with which to address their concerns. As an example, the page has a listing of all JPEO-CBD IT programs. The titles on that listing are linked to the associated Level II web page when available. The page also allows users to access the following information or capabilities:

- Submit a CSR
- Check the status of a CSR

- Manage password and preferences for the web page and the CSR software (Remedy)
- Links to other pertinent Chem-Bio websites and Help Desks.
- For Programs maintaining status and disposition of CSR's on the CBD IT Help Desk infrastructure
 - * Access Frequently Asked Questions (FAQs)
 - * A knowledge base of known issues and fixes
- For Programs with participating Level II operations
 - * Download the latest version, or patch, of program software (e.g. JEM or JWARN)
 - * Download User Manuals for program software
 - * Access training products for supported programs
 - * Read Lessons Learned from other Warfighters

The CBD IT Help Desk is now here, providing a single point of access for the Warfighter to obtain needed help, in the most efficient way possible.

For more information, please contact John Mac-Crossen at macrosen@spawar.navy.mil or Pat Lowe at plowe@spawar.navy.mil.

HELP DESK CONTACT INFORMATION

PHONE NUMBER

1-877-328-0371
619.524.4684
524.4684 (DSN)

EMAIL

metoc@spawar.navy.mil

WEB SITE

The Help Desk's web site is accessed at:
[https://
sskc.spawar.navy.mil](https://sskc.spawar.navy.mil)

Standards and Policy

(Continued from page 7)

SSA Standards and Policy also supports acquisition activities for software intensive systems. We are wired into the Army's and OSD's software acquisition and systems engineering initiatives and are trying to translate these programs into effective practices that benefit JPMs, be it training, process improvement, software architecture design and analysis, or enterprise system engineering plans.

Standard processes, interfaces, guidelines, protocols, syntax, artifacts, data, metrics and templates are being collected in a repository, as an asset JPMs can use for reusable content and examples of items that they will have to produce. This is a work in progress. The repository is located on the JPEO-CBD Integrated Digital Environment (IDE) website (<https://jpeocbd.altess.army.mil>). Check it out and let us know how we're doing, what's missing, whether or not you find your way around, and, in general, how we can help you do your job better and more easily.

For more information, please contact Dan Reuben at dreuben@spawar.navy.mil.

Data Management

(Continued from page 6)

utilize the data model in an open forum. These papers and associated briefings can be found on the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Integrated Digital Environment (IDE) website. They are located under Software Support Activity/Data Management/CBRN Data Model Papers directories.

In addition, our Data Initiative Team recently released the CBRN Data Model Version 1.3. This new version includes most of the Hazard Prediction and Assessment Capability (HPAC) 4.0.4 variables, chemical and biological sensor data structures to support the JPM Guardian program, some Joint Warning And Reporting Network (JWARN) model extensions, population representation, and US MOPP levels, among other items. A number of entities and attributes have been remodeled to more tightly integrate with the Joint Consultation, Command and Control, Information Exchange Data Model (JC3IEDM) and to eliminate potential duplication. In addition, discovery metadata has been implemented at the row level.

The CBRN Data Model and associated documentation can be found on both the JPEO-CBD IDE and JPM - IS websites. If you would like to be added to the distribution list or to obtain a copy of the ERwin data file, please have your government sponsor contact Professor Tom Johnson via email at thjohnso@nps.edu.

For additional information please contact Bill Snee at wsnee@msiac.dmsi.mil

The CBRN Data Model and associated documentation can be found on both the JPEO-CBD IDE and JPM - IS websites.

Science and Technology

(Continued from page 6)

Markup Language) schema, and established interoperability rules between the medical namespace and the CBRN namespace. This would facilitate interoperability between the various COIs, allowing them to achieve the goal of a net-centric data strategy. The second concept, net-ready sensors, would focus on interoperability between legacy sensors and new wireless technology, improving the management of chemical-biological sensors in a net-centric architecture.

With the many proposed development efforts being considered and a growing interest in managing the health and safety of the American populace, a new age of enterprise-level information management is upon us. Our intent is to be on the cutting edge of development, with an eye to rapid transition.

For more information, please contact LorRaine Duffy at lorraine.duffy@navy.mil.

Configuration Management

(Continued from page 8)

User Guide for accessing JCBRND architecture and data products.

In addition to the posting of the CBRND architecture and data products on the IDE website under purview of the JCBRND CMP, formal releases of these products are posted as follows.

CBRND Products	Repository	Release Authority
DoDAF Views	DoD Architecture Repository	JRO-CBRND
DoDAF Views	Knowledge Management (KM) / Decision Support (DS)	JRO-CBRND
CBRN Data Schema	DoD XML Metadata Registry	JPM IS Data Team

For more information, please contact Denise Milligan at dmilli@spawar.navy.mil.

**JPEO-CBD
SOFTWARE
SUPPORT
ACTIVITY**

SPAWAR Systems Center
San Diego (SSC San Diego)
Code 246207
53560 Hull Street
San Diego CA 92152-5001

Phone: 619-553-5410
Fax: 619-553-6902
E-mail: douglas.hardy@navy.mil



We're on the Web!

JPEO-CBD IDE
<https://jpeo-cbd.alfess.army.mil>

JPM IS ITS
<https://jpm-is.spawar.navy.mil>

[both websites require a user account. The JPM IS ITS requires a PKI Certificate]

Contents of the SSA Information Technology Update newsletter are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or the U.S. Navy.

Feedback and suggestions for this newsletter are always welcome.

Please contact:
Dick Brimson
619-553-0806
rbrimson@spawar.navy.mil

Promoting the Interoperability and Integration of CBRND Systems for the Warfighter

The SSA is a user support organization that is funded by the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) and reports to JPEO-CBD via Joint Program Manager Information Systems (JPM IS). It spans and supports all JPEO-CBD Joint Program Managers (JPMs) and Directorates. It is a comprehensive and cost effective single point of contact for users (Customers, Developers, and Warfighters) to receive professional and timely assistance with all CBRN Defense program standards, interoperability, and supportability needs to ultimately facilitate the creation of more efficient, common, and consistently superior interoperable and integrated CBRN systems to the Warfighter.

Interoperability is a puzzle.
We look forward to your piece



The SSA Team



Director - Kevin Adams
858-537-0198
kevin.adams@jpmis.mil
Manager - Doug Hardy
619-553-5410
douglas.hardy@navy.mil
Deputy Manager - Dick Brimson
619-553-0806
rbrimson@spawar.navy.mil

Architecture
Lead - Dave Godso
703-989-0779
godso@spawar.navy.mil
Bill Frame
619-553-0722
bframe@spawar.navy.mil
Josh Pressnell
703-365-9662
joshua.pressnell@rti-world.com
David Rousseau
619-553-9221
david.rousseau@navy.mil

Data Management
Lead - Bill Snee
703-933-3381
wsnee@msiac.dmsomil
Dave Snee
703-933-3342
dsnee@msiac.dmsomil

Information Assurance
Lead - Guy Casciola
619-553-1145
casciola@spawar.navy.mil
CK Kwiatkowski
619-553-5382
candy.kwiatkowski@navy.mil
Blake Lomprey
619-553-9203
blomprey@spawar.navy.mil

Integration & Test
Lead - Jennifer Park
619-553-2848
jennifer.park@navy.mil
Jeff Steinman
858-531-0643
steinman@warpiv.com
Wally Walters
619-553-4013
walwal@spawar.navy.mil
Nathan Delane
540-663-9426
ndelane@egginc.com

Science & Technology
Lead - LorRaine Duffy
619-553-9222
lorraine.duffy@navy.mil

Standards & Policy
Lead - Dan Reuben
301-580-9127
dreuben@spawar.navy.mil
Hiekeun Ko
619-553-8013
hiekeun.ko@navy.mil

Help Desk
Lead - John MacCrossen
619-553-3266
macrozen@spawar.navy.mil
Pat Lowe
619-553-7954
plowe@spawar.navy.mil

Configuration Management
Lead - Denise Milligan
619-767-4191
dmilli@spawar.navy.mil
Connie Miller-Mathews
703-365-9662
cmathews@spawar.navy.mil

Admin Assistant
Peggy West
619-553-6899
pwest@spawar.navy.mil

East Coast Fax: 703-365-9818
West Coast Fax: 619-553-6902

REPORT DOCUMENTATION PAGE

*Form Approved
OMB No. 0704-01-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden to Department of Defense, Washington Headquarters Services Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 06-2006		2. REPORT TYPE Final		3. DATES COVERED (From - To) 1 April 2006 to 30 June 2006	
4. TITLE AND SUBTITLE SOFTWARE SUPPORT ACTIVITY INFORMATION TECHNOLOGY UPDATE NEWSLETTER Third Quarter, FY 2006				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHORS D. R. Hardy J. MacCrossen B. Snee D. Milligan D. Reuben G. Casciola P. Lowe Alion Science SAIC RTI J. Park D. Brimson L. Duffy CSC SSC San Diego				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SSC San Diego Ricciardi Technologies, Inc. Alion Science Computer Sciences Corporation San Diego, CA 92152 8306 Rugby Road 1901 N. Bearegard Street 4045 Hancock Street Manassas, VA 20111 Suite 400 San Diego, CA 92110 Sciences Applications International Corporation 4015 Hancock Street San Diego, CA 92110				8. PERFORMING ORGANIZATION REPORT NUMBER TD 3215	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Space and Naval Warfare Systems Command 4301 Pacific Highway San Diego, CA 92110-3127				10. SPONSOR/MONITOR'S ACRONYM(S) SPAWAR	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES This is the work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction. Many SSC San Diego public release documents are available in electronic format at http://www.spawar.navy.mil/sti/publications/pubs/index.html					
14. ABSTRACT This periodical provides a collection of articles written by the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) Software Support Activity (SSA) as a consistent method of communicating SSA efforts and vision, while providing awareness of key enterprise challenges. The JPEO-CBD is managed by the Space and Naval Warfare Systems Center San Diego and is directed by the Space and Naval Warfare Systems Command. The SSA is a team composed of government and contractor agencies that provide enterprise support in the key tenets of net-centric operations to U.S. Department of Defense chemical and biological programs.					
15. SUBJECT TERMS Mission Area: Information Technology software support net-centricity interoperability information assurance chemical/biological defense data modeling integration joint operations					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			D. R. Hardy
U	U	U	UU	22	19B. TELEPHONE NUMBER (Include area code) (619) 553-5410

INITIAL DISTRIBUTION

20012	Patent Counsel	(1)
21502	Archive/Stock	(1)
21511	S. Baxley	(1)
21512	Library	(1)
246207	D. Hardy	(2)

Defense Technical Information Center
Fort Belvoir, VA 22060-6218 (1)

SSC San Diego Liaison Office
C/O PEO-SCS
Arlington, VA 22202-4804 (1)

Center for Naval Analyses
Alexandria, VA 22311-1850 (1)

Government-Industry Data Exchange
Program Operations Center
Corona, CA 91718-8000 (1)

Approved for public release; distribution is unlimited.