IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 4 Number 1

SPACECOM

Revising the DoD INFOCON System

also inside—

- Combined Endeavor
- DIAP Update
- Biometrics Technology

contents

on the cover

ia initiatives

in each issue

IAnewsletter

Editor
Robert J. Lamb
Creative Director
Christina P. McNemar
Information Processing
Robert F. Scruggs
Inquiry Services
Peggy O'Connor

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

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

Robert J. Lamb
Director, IATAC
703.289.5454

We welcome your input! To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

IATAC
ATTN: Christina P. McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5467
STU-III 703.289.5462

E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Cover and newsletter designed by Christina P. McNemar

Revising the DoD INFOCON System

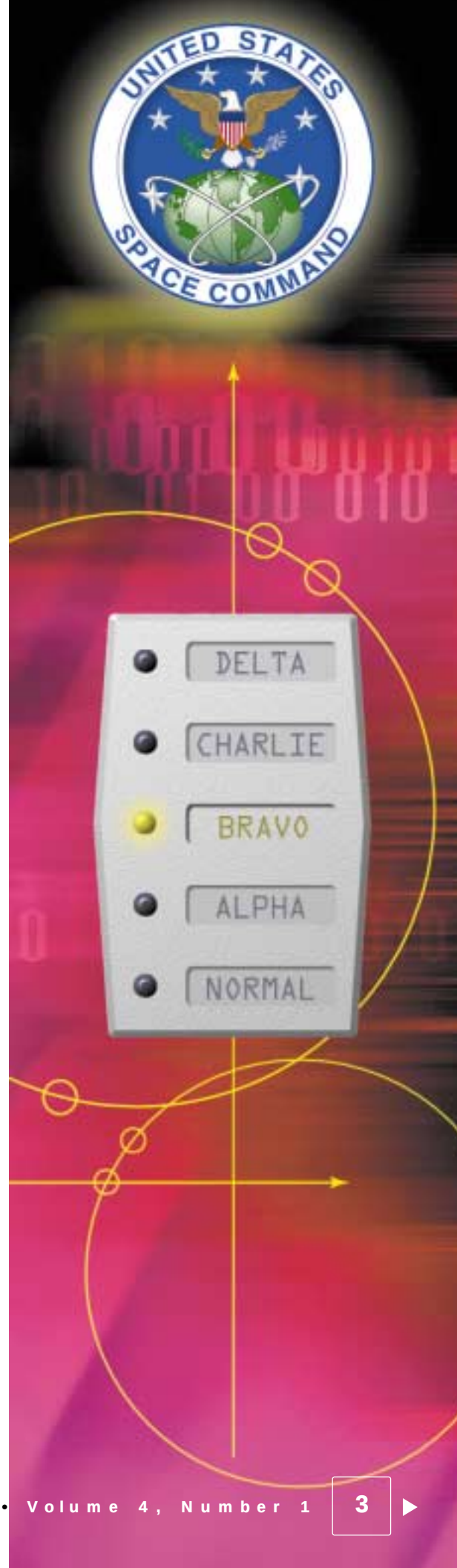
Information Operations Condition

by Ms. Jill Sarff

In the face of an ever growing and sophisticated threat to DoD information networks, the Chairman of the Joint Chiefs of Staff (CJCS) directed the implementation of the DoD Information Operations Condition (INFOCON) system (Chairman's Memorandum CM-510-99, 10 March 1999). In the 18 months since the INFOCON system was established, commanders and network administrators across DoD have applied this new guidance in both exercise and real-world environments. These applications have generated a number of recommendations for enhancing the current INFOCON process. This article addresses the in-work efforts of U.S. Space Command (USSPACECOM) to formulate lessons learned into a "new and improved" INFOCON system. Specifically, it will briefly describe the current INFOCON system, and the activities and processes upon which USSPACECOM has focused.

The DoD INFOCON system provides a structured, operational approach to uniformly heighten or reduce defensive posture, defend against unauthorized activity, and mitigate sustained damage to the Defense Information Infrastructure (DII). The INFOCON system is somewhat analogous to other DoD alert systems, such as Defense Condition (DEFCON) and Threat Condition (THREATCON). These alert systems are all comprised of systematic processes that ensure DoD entities are synchronized in their defensive efforts. Commanders at various levels, depending on the alert system, have the authority to declare condition levels that, when implemented, significantly enhance the protection and defense of personnel, mission operations, and equipment. The INFOCON system, by providing an alert framework for information networks, supports a commander's operational requirement to attain and maintain information and decision superiority.

On 1 October 1999, the Commander, USSPACECOM (USCINCSPACE), assumed command of a brand new mission area, DoD-Computer Network Defense (CND). Also effective the same date, the Secretary of Defense (SECDEF) delegated to USCINCSPACE the authority to declare DoD INFOCON levels. Associated with this important declaration authority was the responsibility, in support of the Joint Staff, to administer the current system and to initiate improvements to the structure and/or processes. Based on feedback from elements across DoD, USCINCSPACE directed a thorough review of the INFOCON system, with specific direction to "standardize and operationalize" the current structure. In response, US-



SPACECOM has initiated the task of reviewing the current INFOCON process and developing recommendations to achieve a more comprehensive, standardized, and responsive INFOCON system.

The current DoD INFOCON system is comprised of five levels declared in order of increasing defensive posture—NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. DoD guidance empowers commanders at all levels to declare INFOCONs for networks within their area of command. Their declared level must remain equal to or higher than DoD's INFOCON level. In addition, current CJCS guidance presents a list of criteria that characterizes each INFOCON level. It also recommends defensive measures to be similarly considered. It is each commander's prerogative to use (or not use) the measures on this list as they see fit in order to direct the specific implementation measures associated with each change in INFOCON level.

In an effort to better understand and share the processes by which commanders across DoD implement the INFOCON system, USSPACECOM hosted a worldwide INFOCON conference in Colorado Springs in June 2000. All Commanders-in-Chief (CINCs) and military Services, and most DoD Agencies were represented at the conference. Each participating organization briefed their local implementation procedures, presented concerns over the current system, and provided recommendations for improvements. In addition, the conference attendees divided into three focus groups in order to concentrate on specific INFOCON elements. The three groups were—

- Commanders' Assessment Criteria
- Directed Actions
- Operational Reporting

USSPACECOM has continued to develop these concepts in its revision effort. The following paragraphs describe each of these focus areas in more detail.

Commanders' Assessment Criteria

The purpose of this focus area in the revision process is to provide commanders with broad guidance on determining an "appropriate" INFOCON level given a combination of operational, threat, and network status factors. As mentioned, the current INFOCON guidance lists general attributes of each INFOCON level. Feedback and operational observations have indicated that more focused guidance for determining INFOCON levels would be helpful. The recent *Love Bug* virus reflected the need for more refined indicators. This worldwide incident elicited a range of INFOCON responses across DoD—from INFOCON NORMAL all the way through INFOCON DELTA (the DoD INFOCON level remained at NORMAL). This observation is not meant to imply that all commanders should have necessarily come to the same INFOCON "conclusion" given a common threat. Commanders retain the authority and responsibility to declare the most appropriate level, given their specific situation. However, it did appear that units in generally similar operational environments interpreted their position within the INFOCON guidance quite differently. Therefore, in order to guide commanders toward a more common application of INFOCON levels, USSPACECOM has developed a matrix which incorporates operational, threat, and network environment factors to help guide commanders toward an INFOCON declaration. It must be emphasized that the intention of this matrix is to provide a decision support tool for commanders. The tool is meant to guide commanders' decisions, not dictate solutions to them. Only the declaring commander has the comprehensive situational awareness to make the most appropriate INFOCON determination for their command.

Directed Actions

A sizeable portion of recommendations for improvement focused on the fact that the current INFOCON guidance recommends (versus directs) defensive measures to be implemented at each INFOCON level. While it is true that local commanders must retain the authority to direct the activities over the networks within their command, the fact that there are no required, standard measures makes it difficult to establish or communicate a "minimum baseline" of measures across the DII. Under the current INFOCON guidance, disposition of the networks within one commander's domain at INFOCON ALPHA may look entirely different than another commander's who has also declared INFOCON ALPHA. Commanders may currently take all, some, or none of the actions recommended at each INFOCON level. The intention of the re-

vised INFOCON guidance is to establish a set of mandatory measures for implementation at each INFOCON level. These mandatory measures will in no way provide all-encompassing guidance for all INFOCON scenarios. As required, USCINCSPACE and/or local commanders will direct additional measures that are specific to the current threat/situation. Rather, a standard set of actions associated with each INFOCON level will ensure a minimum level of uniform activity across the DII when an INFOCON level change is declared. In addition, a set of standard measures promotes an efficient and common understanding across DoD of what minimum actions are being implemented when another commander directs a change in INFOCON levels.

Operational Reporting

The INFOCON system is a structure that is declared and implemented by commanders. This includes operational commanders, as well as Service chiefs (or directors, in the case of DoD agencies) of information networks. Therefore, the messages declaring changes to INFOCON levels, or reporting the status of INFOCON-related activities must be reported through command channels. The efforts to standardize and operationalize the reporting process are focusing on defining operational reporting flows, developing message formats, and identifying timelines required for efficiently reporting INFOCON-related information to the appropriate organizations. The guidance currently being drafted includes the use of operational reports (OPREPs) to report changes in INFOCON levels, and situation reports (SITREPs) to provide operational assessments and status of networks and activities associated with changes to INFOCON levels.

USSPACECOM has recently completed producing a draft version of revised INFOCON guidance. A few issues are currently being coordinated with USCINCSPACE's operational arm for CND, the Joint Task Force for Computer Network Defense (JTF-CND). Following this, USSPACECOM will forward a draft version to the Joint Staff for initial DoD coordination.

The task of continuing to evolve the DoD INFOCON system is a major challenge, given the enormous variety of missions that DoD information networks support, as well as the variety of users, data, and equipment that comprise the information networks. Because of the rapidly changing environment in which these networks operate, the INFOCON system must continue to evolve to effectively respond to threats against DoD networks. USSPACECOM is working to meet this challenge by producing improved guidance for all commanders across DoD and the networks they command and control.

The statements in this document describe work in progress within U.S. Space Command/J39, and do not necessarily represent the official policy of U.S. Space Command, or of the Commander, U.S. Space Command.

Jill Sarff supports the Computer Network Defense mission for U.S. Space Command (USSPACECOM)/J39 as a Systems Engineer. She may be reached at sarffj@usspace.cas.spacecom.af.mil or 719.556.889.

Combined Endeavor '00

by Mr. Kent Waller

"I will not allow you to access our networks!"

bellowed one of the international senior delegates. My reaction was as subdued and casual as I could make it, as I had anticipated that the subject of information assurance (IA) might not go over all that well. I was addressing the Chief Delegates from 35 nations at the Combined Endeavor 2000 (CE 2000) Initial Planning Conference in Tblisi—the capital city of the former Soviet Republic of Georgia. My topic happened to be the first briefing on IA that most of these delegates had ever heard. Speaking in a deliberately slow and steady tone for the interpreters, I figured that at least one of the delegates would understand enough to feel a little insecure about U.S. representatives conducting vulnerability assessments on their networks. The delegate's retort sparked a lively debate, and I had to retreat to my fallback position—a menu of voluntary self evaluations, training, and demonstrations.

Despite this somewhat rough initial briefing, I was thrilled to be there. Combined Endeavor, after all, is the world's largest multinational tactical communications exercise. This annual exercise is sponsored and coordinated by Headquarters United States European Command's Command, Control, and Communication (C3) Directorate (ECJ6). More than 650 military personnel from 35 nations participated in Combined Endeavor 2000 held in Lager Aulenbach, Germany May 11-25, 2000.

Participating countries included Albania, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Macedonia (FYROM), Moldova, Norway, Poland, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Netherlands, Ukraine, United Kingdom, United States and Uzbekistan. NATO also participated.

My goal during this exercise was to educate our potential future partners about the importance of IA. Additionally, I hoped to collect data to perform a very simplified IA evaluation of the "coalition" network that we would build in the CE 2000 Information Systems testbed. I felt this information could be useful to our new partners in understanding the importance of IA and to our coalition commanders in understanding what types of vulnerabilities we might encounter in coalition IA.

Clearly, one of the first hurdles was the issue of trust among the participating nations. During that first meeting in Tblisi, I was looked at with quite a bit of suspicion—regarded as though I must have

some hidden agenda. But my briefings became more palatable and I became more familiar to the delegates throughout the course of three planning conferences. By the time the exercise finally began, many of the delegation chiefs were completely focused on the importance of IA in coalition networks. I was no longer "the lecturer"—instead, I was kept busy answering questions from interested individuals. In response to these queries, and since this was primarily a communications interoperability exercise, I kept pitching an underlying theme—that failure to communicate, for whatever reason, is failure to interoperate, and lack of basic system protection mechanisms can lead to a failure to communicate. Of course, another important aspect of gaining trust occurs outside of the conference room. Informal discussions and a friendly handshake can do as much to alleviate fear and mistrust as any good briefing.

Within the Information Systems (IS) test cell area of the exercise, I was able to work closely with the subject of IA while witnessing the testing of our coalition's ability to exchange and conduct simple command and control oriented E-mails, formal message traffic, file transfer protocol (FTP) transactions, and Hyper Text Transfer Protocol (HTTP) Web transactions. I also used the testbed as a forum for technical presentations and demonstrations on subjects such as firewalls, public key infrastructure (PKI), intrusion detection, viruses, and hackers.

Within this test cell we had a fascinating array of participants. There were several countries with high-end command and control systems. Some countries came with truck mounted or deployable tactical networks. One country had workstations connected remotely over a secure high frequency (HF) link. And one country participated in the IS test cell with a single young officer who could barely speak English, having only a laptop, a network interface card (NIC) and an eagerness to interoperate.

Most of the nations in the IS test cell agreed to help in the IA evaluation by having an IA officer complete two self evaluation forms (one for workstations and one for servers) which I had put together earlier. The forms were very simple in nature and were kept completely anonymous so that no one country would feel that the U.S. IA guy (that would be me) was evaluating their networks for intelligence purposes. The results of these evaluations were used to complete a very simplified risk analysis. I put this analysis together primarily to demonstrate how a simple risk analysis could be accomplished, but also to help all players gain a limited understanding of where our coalition IA shortcomings may be. The results are provided in Tables 1 and 2.

High Threat: ■ ≤ 85%, ■ 86% – 99%, ■ =100%
Medium Threat: ■ ≤ 50%, ■ 51%–85%, ■ ≥86%
Low Threat: ■ ≤ 25%, ■ 26%–50%, ■ ≥51%

	Threat	Countermeasure (CM) Planned	% of WS using CM
High	Viruses	Antivirus Software	85%
	Hacker	Secure Logon	87%
		No Internet Access	95%
	Power Disruption	UPS	77%
	HVAC Failure	Backup Procedures	28%
		Hardened System	49%
Medium	Insider Data	Access Control	49%
	Sabotage	Screensaver Password	92%
	Data Compromise	Secure Logon	87%
	(electronic)	Access Control	49%
	Hardware	Backup Procedures	28%
	Failure	UPS	77%
Low	Software Failure	Backup Procedures	28%
	Theft	Restricted Access	100%
		System Inventory	69%
	Data Compromise	Restricted Access	100%
	(non-electronic)	Trained Personnel	85%
	Attack/Bomb	Posted Procedures	41%
	Fire or Smoke	Posted Procedures	41%
	Other Disasters	Posted Procedures	41%

Table 1. Information Systems Test Cell Risk Analysis on 39 Workstations (WS).

	Threat	Countermeasure (CM) Planned	% Systems using CM
High	Viruses	Antivirus Software	71%
	Hacker	Secure Logon	100%
		No Internet Access	100%
	Power Disruption	UPS	79%
	HVAC Failure	Backup Procedures	57%
		Hardened System	57%
Medium	Insider Data	Access Control	86%
	Sabotage	Screensaver Password	86%
		Auditing Engaged	86%
		Audits Reviewed	43%
	Data Compromise	Secure Logon	100%
	(electronic)	Access Control	86%
	Hardware	Backup Procedures	57%
	Failure	UPS	79%
Low	Software Failure	Backup Procedures	57%
	Theft	Restricted Access	100%
		System Inventory	93%
	Data Compromise	Restricted Access	100%
	(non-electronic)	Trained Personnel	100%
	Attack/Bomb	Posted Procedures	60%
	Fire or Smoke	Posted Procedures	60%
	Other Disasters	Posted Procedures	60%

Table 2. Information Systems Test Cell Risk Analysis on 14 Servers.

Two of the statistics which I found striking were that only 79 percent of servers had an uninterrupted power supply (UPS) in operation and only 57 percent of servers utilized data backup and recovery systems. Additionally, only 77 percent of workstations had UPS and only 28 percent of workstations had data backup and recovery systems. In deployed environments such simple oversights can have critical mission impact!

These results were passed to the participating nations in the IS test cell for their own informational purposes. Before the exercise concluded one foreign officer told me that he had already provided the report to his senior commander and they were acting to improve their IA posture. I received another indicator of successful delivery of the IA message at the closing ceremony, where German Rear Admiral Klaus-Peter Hirtz made strong statements regarding the importance of IA in coalition operations.

Given this, I believe that in coming years Combined Endeavor will provide us with continuing opportunities to test and evaluate new IA concepts in coalition networks. We need to continue to educate and assess our current capabilities, but we also need to work towards a common international solution set for coalition networks oriented towards handling a more sensitive level of command and control. Colonel Treece, USA, in the Spring 1999 IAnewsletter, discussed a "Coalition Secret" level network that all partners could share. We need to use future Combined Endeavors as a staging platform to address the associated issues of encryption, authentication, and verification that should accompany such a network. This initial Combined Endeavor 2000 IA effort has successfully laid a strong foundation for these types of future activities by establishing a baseline level of understanding and trust.

Mr. Kent Waller is an information assurance program manager for HQ United States European Command. He earned his B.S. in engineering from the University of Oklahoma in 1986 and his Master of Public Administration from the University of Oklahoma in 1990. He may be reached at wallerkl@eucom.mil.

DIAP Update

Defense-wide Information Assurance Program

by CAPT J. Katharine Burton, USN

The Defense-wide Information Assurance Program (DIAP), established in 1998 by the Deputy Secretary of Defense, has continued to mature in executing its responsibilities as the organization responsible for coordinating, integrating and ensuring a consistent and coherent Information Assurance (IA) program across DoD. Since its inception, the staff of the DIAP has made considerable progress in not only documenting what the CINCs/Services/Agencies are doing in IA, but also in providing advocacy for these programs both within and without the Department. The organizational structure has undergone a few changes also, reflecting a more in-depth understanding of how to execute the mission with minimal resources. Figure 1 illustrates the current organizational structure of the DIAP.

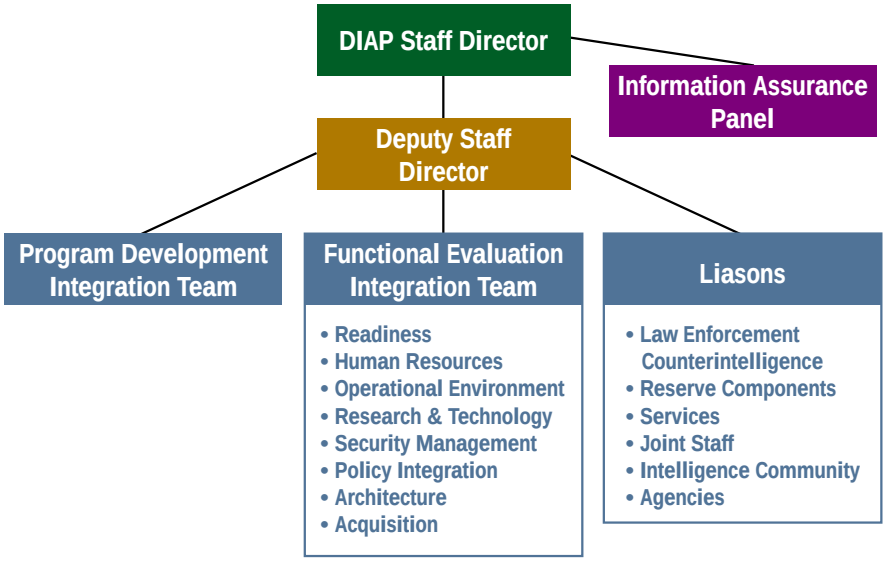
There are a number of areas where significant progress in addressing DoD IA issues have been made. In this article, four of these areas will be addressed. In future articles, additional areas will be discussed. The four areas are: Human Resource Development, Readiness Assessment, DoD Public Key Infrastructure (PKI) Program, and Counterintelligence/Law Enforcement.

Human Resource Development

The Human Resource Development functional area of the DIAP was established to develop ways to improve the recruitment and retention of adequately trained IA personnel resources required to carry out the Department's defensive information operations (DIO), and to provide oversight of implementation plans towards that end. The Department conducted an IA and information technology (IT) Human Resources Integrated Process Team (IPT) study for six months. The IPT analysis produced major findings which, when implemented, will greatly improve how the Department manages IA/IT billets and personnel. Generally, it was found there is no Department-wide recognition of the very real and growing threat to our warfighting capability as evidenced by inadequate priority, funding, training, and focus on information assurance. The most significant finding was that IA and IT Management personnel readiness is more problematic than simply providing training opportunities and financial/career incentives to IT professionals. The IPT final report produced 19 recommendations to be implemented over a five-year period with a cost factor of approximately $64 million. A memorandum to implement these recommendations was signed by the Deputy Secretary of Defense (DEPSECDEF) on 14 July 2000 and the implementation planning process has begun.

Once implementation plans have been developed and promulgated, members of the DoD Human Resource Development Working Group will provide guidance and oversight within their respective DoD organizations. This group is composed of IA representatives selected under the auspices of the Military Communications Electronics Board's (MCEB) Information Assurance Panel (MCEB is chaired by Joint Staff J6).

Future plans for the DIAP Human Resource Development functional area include looking at other IA professional training and certification requirements



not covered in the recently concluded IPT. Additional emphasis will be placed on developing IA training for all DoD and the identifying appropriate methods of distributing that training.

Readiness Assessment

The Readiness Assessment Functional Area of the DIAP has created a team that has begun developing a capability to assess the IA Readiness status of the DoD IT systems. When fully developed and deployed, this capability will allow the DoD to measure and observe their effectiveness in applying IA resources and respective practices and procedures to protect, defend and operate the Department's vast IT resources and capabilities throughout all phases of conflict.

As conceptualized, the assessment capability will consist of high-level, indexed metrics that will present a "big picture"view of the DoD IA Readiness status. The indexed metrics will consist of aggregated lower-level metrics, some of which will consist of lesser-level metrics. This hierarchical approach to metrics will provide the DoD with a capability to "drill down" to levels of detail appropriate for action by respective levels of management. The metrics will be developed collectively by IA personnel, with inputs from operational mission owners affected by the metrics.

To accelerate development of the metrics segment of the IA Readiness assessment capability, the DIAP, in conjunction with the Information Assurance Panel, recently established an IA Readiness Metrics Working Group. Membership and active participation in the working group is encouraged of all DoD Components.

As part of its overall effort to develop a comprehensive IA Readiness Assessment capability, the Readiness Assessment Functional area will identify processes and methodologies for collecting, submitting, aggregating, reporting, and analyzing applicable metrics data. In its end-state, the IA Readiness Assessment capability will be institutionalized through DoD policy as an integrated process, and will be iteratively reviewed and modified as required.

The IA Readiness Assessment team has been busy visiting and briefing Components to encourage all Components to participate in the working group, and is now expanding its efforts to include informing other government agencies through briefings, conferences and workshops. Information and contact information for the IA Readiness Metrics Working Group is readily available from the DIAP.

PKI Activity

There are a number of activities occurring in the DoD PKI program. This article will give a quick run-through of some of the most significant activities. The DoD PKI recently transitioned successfully to the Class 3.0 Release 2 infrastructure. Although the process for obtaining a Release 2.0 certificate is the same as that of Release 1.0 (also known as DoD Medium Assurance PKI Pilot certificates), Release 1.0 certificates may continue to be issued until 31 December 2000 to support any ongoing operational needs. If a Release 1.0 certificate is misplaced after 31 December 2000, it must be replaced with a Release 2.0 certificate. However, a user of DoD PKI Release 1.0 should be aware of a few issues (listed below) when planning a transition to Release 2.0. Release 1.0 certificates will be valid until they expire, 3 years after issue. The Release 1.0 infrastructure will stay in place until 31 December 2003 only for maintenance of Release 1.0 certificates created prior to 31 December 2000.

A Front End Assessment (FEA) of the DEERS/RAPIDS/Common Access Card/PKI integration has been completed. The FEA permitted the DoD PKI PMO to establish revised milestones for DoD PKI fielding. These new milestones have been incorporated into a revised DoD PKI Policy Memorandum dated 12 August 2000.

The DoD Class 3 Interoperability Test Facility has been recently established at the Joint Interoperability Test Command (JITC) in Fort Huachuca, Arizona. The facility has been designed to test PKI applications to insure their interoperability with the DoD PKI. In concert with this activity, the National Institute of Standards and Technology (NIST) is developing a generic set of test procedures to test the certificate path validation process. These generic procedures will be posted on a NIST web site and be made available to all communities. JITC will tailor the generic procedures to the specific application and perform the interoperability test.

The DoD PKI PMO conducted a DoD PKI Users' Forum on 12-13 September 2000 in Las Vegas, Nevada. The forum reached a capacity of 600 plus attendees, including featured keynote speaker, the Honorable Mr. Art Money. Presentations included a DoD Smart Card Information Briefing, Interoperability Testing, DoD Target Class

4 Briefing, Intelligence Community PKI, and PKI applications. A technical panel also led a discussion about commercial applications (Netscape and Outlook) currently being used in the DoD PKI.

Law Enforcement and CI Support to IA

The Law Enforcement (LE) and Counterintelligence (CI) communities provide critical support to the Department's IA Defense-in-Depth strategy. The LE/CI community is usually going to be the first responders to any criminal, terrorist or counterintelligence attack on our DoD systems. Before senior decision-makers can decide on the appropriate response to an incident, attribution for the attack must be established. Because attacks are usually routed through U.S. systems, law enforcement is critical to the collecting of information, working backwards to the origin of the attack. Using search warrants, subpoenas, consensual and legal non-consensual wiretaps, witness interviews and sources (informants), law enforcement and the counterintelligence communities gather information that lead back to the origin of the attack. Once attribution for an attack has been established, a course of action can then be determined.

The information gathered during the intrusion investigation must be gathered legally as well as in a manner that will properly maintain chain of custody to preserve the integrity of the evidence, because in the overwhelming majority of cases, the subject of the attack, when identified, will be prosecuted. Active and aggressive law enforcement can also deter attacks by making it too risky for the perpetrators. The DoD Law Enforcement and Counterintelligence communities have taken several significant steps in FY 2000 to better provide this critical support for IA.

Law Enforcement & CI Center for CND

DoD Directive 8530-aa, which is currently in coordination, created the Defense Criminal Investigative Organizations Law Enforcement and Counterintelligence Center (DCIO LE & CI Center). This organization coordinates LE and CI investigations and operations supporting Computer Network Defense (CND) and is staffed by all Defense Criminal Investigative and Counterintelligence Organizations (DCIO). DoD Directive 8530-aa formalizes and institutionalizes the LE/CI Cell that is currently co-located with the Joint Task Force for Computer Network Defense (JTF-CND).

The LE and CI Center serves as the primary interface between DoD and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) for CND-related law enforcement and counterintelligence issues. They receive operational direction from the DCIOs and respond to the information requirements of the U.S. Space Command and Components. They coordinate CND investigations and operations among the DCIOs, providing analytical services to support CND investigations and operations and the Common Operating Picture (COP). The DCIO LE and CI Center supports operational decision making by coordinating CND related investigations and operations that cross DoD Component or Federal Department/ Agency bounds, and contributing law enforcement and counterintelligence generated information to a CND COP. All the DCIOs exchange CND related information with the LE & CI Center. The LE & CI Center will maintain an information system providing coordinated information input to the CND COP and to support the operational needs of the DCIOs.

CND–Law Enforcement–Operations Chiefs Working Group

To provide standardized direction, guidance, investigative tools and training among the Defense Criminal and Counterintelligence components we have recently established the Computer Network Defense-Operations Chiefs Working Group (OCWG) composed of senior representatives from each of the Department of Defense Criminal Investigative and Counterintelligence organizations. The OCWG serves to provide this direction, guidance and support to the Joint Law Enforcement and Counterintelligence Center at the JTF-CND.

The OCWG consists of the most senior program/policy manager or representative responsible for the computer investigations and operations program within each of the DCIOs (AFOSI, DCIS, NCIS, USACIDC, ODCSINT):

- Air Force Office of Special Investigations (AFOSI)
- Defense Criminal Investigative Service (DCIS)
- Naval Criminal Investigative Service (NCIS)
- U.S. Army Criminal Investigation Command (USACIDC)
- U.S. Army Office of the Deputy Chief of Staff for Intelligence (ODCSINT)

Associate membership of the OCWG will include, but not be limited to, the organizations

continued on page 15

CND in a Coalition Environment...

Why?

by Major Mike Purcell

That is the simple question asked by some regarding the conduct of Computer Network Defense (CND) in a coalition environment. Do the risks of exposing vulnerabilities not outweigh the potential return? To a large extent, the answer to these questions lies in the fact that, to varying degrees, most allies of the U.S. already share vulnerabilities through the progressively increasing homogeneity of software and hardware used on modern networks. Although the number of networks currently in use by the U.S. and its allies is staggering. There are remarkable similarities among them. Many use similar technologies (if not identical products) to provide intrusion detection, routing, anti-virus protection and application layer services. Most importantly however, there is considerable commonality between operating systems. This has been recognized in the larger governmental and corporate networking world through the establishment in 1990 of the Forum of Incident Response and Security Teams (FIRST, www.first.org). FIRST is an international organization chartered to foster cooperation among its members in the areas of prevention, detection, and recovery from security incidents. It also provides an open forum for discussing current threats and sharing security related information, tools and techniques. It is this type of cooperation that is being pursued between the U.S. Department of Defense (DoD) and the Canadian Department of Defence (DND).

The operational case for cooperation in the realm of CND is strengthened by the recent history of coalition operations. In the past decade alone, U.S. forces have participated in a large number of coalition operations including the Persian Gulf 1990-91, Provide Comfort 1991, Restore Hope 1992-93, NATO Stabilization Force Kosovo 1995-present, Determined Force 1998, Eagle Eye 1998, Determined Guarantor 1999, Allied Force 1999, and Kosovo Peacekeeping Force 1999–present. This is not a complete list; it only covers coalition operations that include Canada, the United Kingdom and or Australia. In the context of ongoing coalition operations with Canada, NORAD must also be included. Here is an example of an integrated command with some integrated networks that span international boundaries. This is clearly a case for the conduct of coalition CND.

Within the context of CND, there are different areas for coordination and cooperation—information sharing, doctrine, vulnerability assessments, warning, research and development, and tactics techniques, and procedures. Existing agreements that either need no modification or need to be amended to include the sharing of CND information, already cover some of these areas. The issue in this case is the development—by both partners—of efficient mechanisms for the rapid production and dissemination of CND-related information.

Another area in which there is considerable commonality is in Information Conditions (INFOCON). Briefly, INFOCONs are a means by which the current threat to DoD or Canadian DND information systems can be categorized and in which guidance on how to counter the threat is provided. Although the system is currently only in use in the DND and DoD, a similar system is in use in the UK. Sharing of INFOCONs will be one of the first concrete examples of information sharing between Canada and the U.S. This cooperation is critical—especially in the NORAD theatre. As much as possible, information concerning the reasons for changes in INFOCON levels will be passed, however, there may well be times where this information may not be shared, depending on its source, or the implication of it.

The formal development of DND/DoD cooperation started in 1999 with a Statement of Intent between Mr. Art Money, the DoD Assistant Secretary of Defense for Command, Control, Communications and Intelligence [OASD(C3I)] and his counterpart in Ottawa, Mr. H. Dixon. The parties agreed in principle that work should begin on a formal CND arrangement between Canada

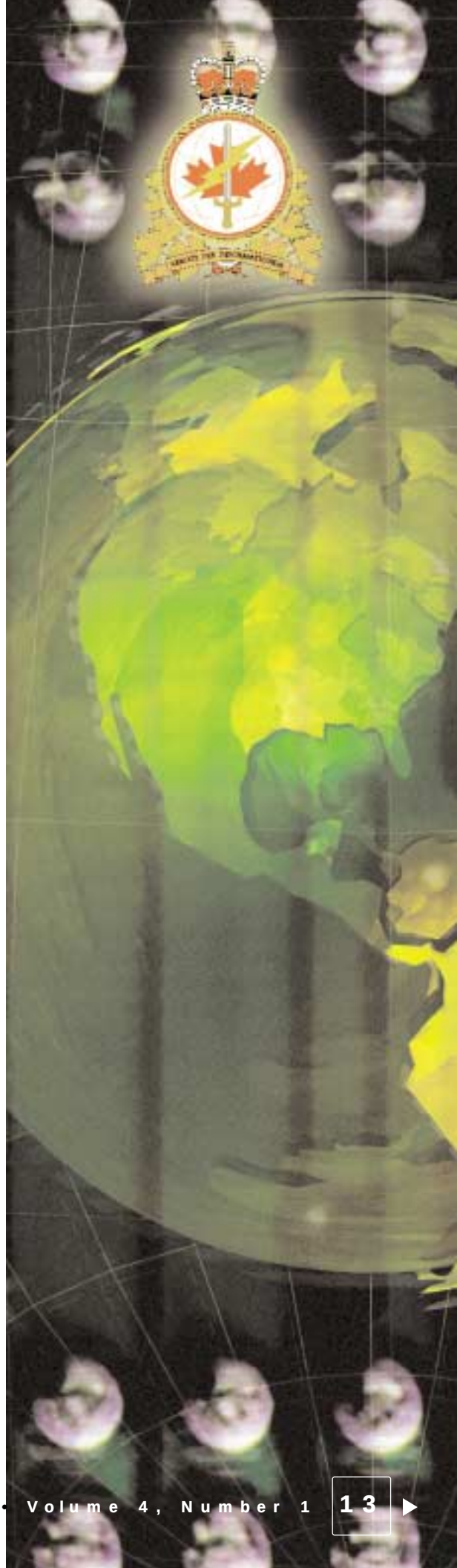
and the U.S. Shortly after this letter was signed, a Canadian exchange officer was posted to the Joint Task Force for Computer Network Defense (JTF-CND) in Arlington, Virginia. His counterpart, a USAF Major, had been on station in Ottawa for about one year. Since that time, work has been progressing at a rapid pace. A draft Memorandum of Understanding is already under development. Concurrent with this work is the development of detailed Standard Operating Procedures (SOP), which will define exactly how DND and DoD intend to perform coalition CND. At the fall meeting of the Information Operations Working Group (the working group assigned by the Military Cooperation Committee to study this issue in detail) the draft SOP was developed to the point that it should be finalized by early in 2001. The primary goal of all of these documents is to share information between the two countries for the purpose of enhancing the CND efforts of both. It is expected that some level of initial operations will be reached by the end of the year. As with all international agreements, this CND agreement will deal with only certain items, all of which will be explicitly delineated.

Depending on the degree of success achieved with this agreement, it is likely that the concept will be extended to other partners. Interestingly, despite the commonality of hardware and software mentioned earlier, the threats to the Defense Information Infrastructure (DII) of each potential partner vary greatly. This difference is directly related to the implementation of the networks and the networks' exposure to the Internet. The implications of this are that each participating nation must have a thorough understanding of each other's structure if they are to be effective in providing early warning. A good example of this is the recent *I Love You* (ILY) virus. Any nation involved in a CND alliance must have a good understanding of the vulnerabilities of its systems. In the case of ILY there were a number of nations whose DII was virtually unaffected. In such a case, those unaffected countries would have had to know that ILY could cause significant damage to one or more of its partners and taken steps to report appropriately (especially if that nation was the first to be hit).

Mr. Timothy Bloechl has led this effort to date on behalf of JTF-CND. CDR Chuck Peirsall from USSPACECOM, and Mr. Robert Simmerly, [OASD(C3I)] have the lead for their respective organizations. In Canada, the staff in the J6 Information Operations Group in National Defence Headquarters, Ottawa has also been of considerable assistance.

While there is a great deal of work left to be done, great strides have already been taken. As with the creation of any international agreement there is a considerable amount of consensus building and staff work to be done.

Major Mike Purcell is a Canadian Army Communications Officer on exchange duty with the JTF-CND. He has completed 1 year of a three year tour. He may be reached at purcellm@jtfcnd.ia.mil.



67th Intelligence Wing Acquires New Mission

Colonel James Massaro, USAF

On 1 March 2000, the Air Intelligence Agency [(AIA) an Air Force Field Operating Agency headquartered at Kelly Air Force Base, Texas] mandated the transfer of selected Air Force Information Warfare Center (AFIWC) (an AIA subordinate unit also headquartered on Kelly Air Force Base) elements to other parts of AIA.

One of the elements that transferred is the Air Force Computer Emergency Response Team (AFCERT). The AFCERT is the single point of contact for the reporting and handling of all computer security incidents and vulnerabilities in the Air Force. The AFCERT, along with other information operations elements, transferred to the 67th Information Operations Wing (a co-located unit also headquartered on Kelly Air Force Base) on March 1.

The AIA realignment called for operationalizing the AFCERT's Computer Network Defense (CND) mission by combining it with other information operations capabilities into a squadron. Thus, the 33rd Information Operations Squadron (33IOS) was formed reporting to the 67th Information Operations Wing's 67th Information Operations Group, 67th Information Operations Wing.

Initially, the AFCERT and offensive information operations were combined into a unit, Detachment 10, 67th Intelligence Group. This detachment supports defensive and offensive information operations to Air Force, Joint and Allied forces by providing trained personnel, technical assistance and operational support.

Detachment 10's AFCERT function is a key component of the Joint Task Force for Computer Network Defense (JTF–CND). The JTF-CND, headquartered at Defense Information Systems Agency (DISA), is responsible for defending the DoD's computer networks. AFCERT is the CND focal point for the Air Force.

As the CND focal point, the AFCERT plans, coordinates, and conducts operations to protect Air Force systems from network exploitation and denial-of-service activities. It deters or prevents an adversary from exploiting or denying authorized users access to Air Force networks and automated information systems. The AFCERT also detects, identifies, and responds to suspicious activities and incidents that may impact Air Force operations and capabilities. Finally, it accesses and reports on the impact of adverse network activity in time for operational commanders to assess and counter intrusions in their operations (see "JTF–CND and AFCERT: Allies in the Information War," *IAnewsletter,* Vol. 3, No. 2, page 13*).*

Detachment 10 is structured similarly to that of other squadrons. It has a Commander, Command Section, First Sergeant, Mission Support and Operations functions.

Although the mission didn't change when Detachment 10 became the 33IOS, there are some new initiatives, including—

- A virus cell for the AFCERT,
- Joint Web Risk Assessment Cell for reporting Web policy compliances,
- Educating the field about the AF Information Operations Condition (a threat condition for information systems),
- Establishing an Air Force level Network Operations, Security Center (NOSC),
- Implementing Common Intrusion Detection Director (CIDD) 3.0 implementation to Major Command NOSCs.

Virus Cell

Due to the threat of viruses and other forms of malicious logic to the security of Air Force networks, the AFCERT incorporated virus support into its daily operations.

The virus cell is the first line of defense for the customer. The cell coordinates countermeasures to contain viruses and restore operational capability to Air Force networks, disseminates virus activity and hoax information, and serves as the Air Force liaison to antivirus commercial vendors and DISA.

Joint Web Risk Assessment Cell Reporting

The AFCERT is working to streamline the reporting and compliance process concerning Joint Web Risk Assessment Cell Operational Security findings on Air Force Web sites. (The JWRAC is a Reserve component team that monitors and evaluates DoD Web sites to ensure they do not reveal sensitive defense information.) This will involve working in conjunction with Air Force Public Affairs, the Air Force Communications and Information Center, and the Air Force Director of Intelligence, Surveillance, and Reconnaissance to formalize procedures establishing the AFCERT as the sole Air Force point of contact. Draft procedures are currently under coordination at the Action Officer level for eventual release as Air Force policy.

The AFCERT fosters close relations with Air Force Public Affairs and Air Force Information Warfare OPSEC experts. These relationships ensure Web sites contain useful public information that does not compromise the Air Force mission.

Information Operations Condition (INFOCON) Education

Air Force Headquarters released an INFOCON implementation policy message in June 1999 outlining the roles and responsibilities of the Air Force Information Assurance and CND communities.

Recommendations and lessons learned have been gathered and included in the drafting of an Air Force INFOCON instruction. The instruction has been sent out for further review and comment.

Steps are being taken to ensure the field understands the INFOCON process. The AFCERT will work closely with USSPACECOM, JTF-CND, and the other services to refine the DoD INFOCON process in the coming months.

Establishment of an Air Force Level NOSC

The Air Force is currently looking into establishing an Air Force-level NOSC. The purpose of the Air Force NOSC would be to provide one-stop support for all CND and IA issues for the Air Force. This will also provide an improved network situational awareness picture for Air Force senior leaders.

Implementing CIDDS 3.0/CDS

In the upcoming months, Air Force Major Command NOSCs will receive CIDDS 3.0/Computer Security Assessment Program (CSAP) Database System (CDS). These new tools will allow major commands (MAJCOMs) to provide real time monitoring of their network areas of responsibility. This in turn, will free AFCERT resources to concentrate on event correlation and command and control issues. Rules of Engagement for this new relationship are currently under development.

The new 33IOS will continue to remain on the cutting edge of technology as the information age unfolds. Like its predecessor organizations, it will be looked to for leadership and guidance in information operations for years to come.

Colonel James Massoro. USAF is the Commander of the 67th Information Operations Wing.

DIAP Update *continued from page 11*

and disciplines listed in Tables 1 and 2.

Table 1. Summary of disciplines represented at the workshop.

Discipline	Number
IA Professionals	127
Criminal Investigators	103
Attorneys	80
Total	**310**

Table 2. Summary of components represented at the workshop.

Component	Number
Army	51
Navy	26
Marines	6
Air Force	141
Joint/DoD Agency	65
Others	21
Total	**310**

As a result of overwhelming feedback, it was decided that the DoD-wide Computer Crime Workshop should be an annual event. The next Computer Crime Workshop is tentatively scheduled for late April or early May 2001. Over the next year, the DIAP will provide updates on these and other programs that are on-going and affect the entire Department. Individuals with questions are encouraged to call or E-mail.

CAPT Burton earned her B.A. in English Literature from the University of Oklahoma and a M.S. in National Security Strategy with a certificate from the Information Strategies Concentration Program at the National War College. She also holds a M.A. in Management Information Systems from George Washington University and is a 1986 graduate of the Armed Forces Staff College. She is the Staff Director, Defense-Wide Information Assurance Program (DIAP), in the Information Assurance Directorate of [OASD(C3I)]. She may be reached via E-mail at Katharine.Burton@osd.pentagon.mil.

Biometrics Technology

From Science Fiction to Science Fact!

by Mr. Jeff Dunn and Mr. Matt King

You sit down in front of your computer and the screen saver instantly unlocks. You touch your laptop and you are instantly logged on. You walk up to an ATM machine, and when you are at arms length it greets you by name and says, "Please select the transaction of your choice." You call a toll free number to place an order and recite your account number, the system approves your purchase, charges your credit card and delivers the product to your home address.

Does this sound like Science Fiction? Well, all of these scenarios are true science fact and are happening today, thanks to the use of biometric technology.

What are biometrics?

Biometrics, in the context of automated access control, are automated methods of recognizing a person based on physiological or behavioral characteristics. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, wrist veins, and others.

Most biometric systems have three main modes of operation: enrollment mode, identification mode, or verification mode. Every biometric system must have an enrollment mode and, while some biometric systems support both identification and verification modes, others may only support one of these modes. During the Enrollment mode, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition can be used in the Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match. For example, an entire database may be searched to verify that a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching.

A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching.

In most computer access or network access environments, verification mode would be used. A user enters an account number, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

Why use biometrics?

Using biometrics for identifying human beings offers some unique advantages. Only biometrics can identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember dozens and dozens of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, E-mail accounts, wireless phones, Web sites, and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, law enforcement has used fingerprints to identify people for nearly a century. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have also come into widespread use. Some newer biometric meth-

ods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is "user-friendliness" of a system. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels or instances of authentication will become less of a burden for users.

What about standards?

An indication of the biometric industry's substantial growth and maturity is the emergence of biometric industry standards and related activities. Industry standards ensure the availability of multiple sources for comparable and competitive products in the marketplace. A number of organizations are currently involved in developing standards for biometrics. See the Biometric Consortium Web site at http://www.biometrics.org/ for more information about these organizations and activities.

What is the Biometric Consortium?

The Biometric Consortium was chartered as a Working Group "to serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification/authentication technology."

The Biometric Consortium now has over 800 members from government, industry, and academia including over sixty different federal agencies. The main benefit of the organization is to share information about biometric technology among the members.

What do I do now?

Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Areas that will benefit from biometric technologies include network security infrastructures, government IDs, secure electronic banking, investing and financial transactions, wireless communications, retail, health services, and social services. In addition, highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global economy. Many technology providers are already delivering biometric authentication for a variety of Web-based and client/server based applications to meet these and other needs. While biometric authentication is not a magical solution that solves all authentication concerns, it is now science fact, not science fiction. Biometric authentication technology is an easier, less expensive, and more secure mechanism for access control that is now a viable solution for a wide variety of applications.

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. He Co-Chairs the Biometric Consortium. Mr. Dunn frequently provides technical advice to government policy makers and has testified as an expert witness before Congressional hearings.

Matt King provides security engineering support for Jeff Dunn's work at the National Security Agency and is the liaison between the National Security Agency and the Biometric Management Office and the United Kingdom's Biometric Working Group.

References

AAMVAnet, Inc. Standards Development Web site: http://www.aamva.org/aamvanet/indexStandards.html

ANSI/NIST-CSL 1-1993, *Data Format for the Interchange of Fingerprint Information*, http://www.itl.nist.gov/iaui/894.03/fing/stand1.html

ANSI/NIST ITL 1-1999 (Draft), *Data Format for the Interchange of Fingerprint, Facial, & Scar, Mark & Tattoo (SMT) Information*, http://www.itl.nist.gov/iaui/894.03/fing/stand2.html

ANSI X9, http://www.x9.org

BioAPI Consortium Web site: http://www.bioapi.org

Biometric Consortium Web site: http://www.biometrics.org

Breitenberg, M.A., Office of Standards Code and Information, NIST, *The Abc's Of Standards-Related Activities In The United States*, NBSIR 87-3576, May 1987.

Common Biometric Exchange File Format Web site: http://www.nist.gov/cbeff

International Biometric Industry Association (IBIA) Web site: http://www.ibia.org

Open Group CDSA Web site: http://www.opengroup.org/security

Teletrust http://www. teletrust.de

Toth, Robert B., Ed., NIST, *Profiles of National Standards-Related Activities*, NIST SP 912.

Information Operations in the Army Reserve

The USAR needs soldiers with "high tech" skills to fill units and positions nationwide.

by Major Greg Williams, USAR

Army Reservists who work in the information technology (IT) industry with their civilian employers are being sought to become the nation's new 21st Century information warriors.

The Department of Defense and the Army are asking the Army Reserves (USAR) to support information operations (IO) at all levels on an ever-increasing basis. Army Reserve soldiers possessing many of the "high tech" skills associated with IO are being actively recruited to fill newly-formed units and positions.

These new units, based at multiple locations throughout the United States, will draw from the entire IT-skilled USAR population, regardless of a soldier's current military occupational specialty.

Public Affairs Unit.

To identify reservists with IT experience, the civilian acquired skills database is used. The database can be accessed by any soldier at http://www. citizen-soldier-skills.com. First, reservists complete a resume and assess their individual skills. Second, the record created by the reservist is added to a searchable database that is used to identify soldiers with needed skills.

Information Operations Defined

Information operations are used to defend our computer systems and to affect an adversary's information systems. The overall objective is to gain information superiority. A primary function of USAR IO units is to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation.

Information operations are not limited to automated systems. They include specialties such as psychological operations, military intelligence, signal, civil affairs, and public affairs. Functions include all forms of operational security, electronic warfare, and computer network defense.

With effective IO our leaders have the information they need, when they need it, in a form they can use to win the fight. This allows commanders to understand complex battlefields, control communications and computers, as well as influence people's attitudes.

They can also interrupt, limit, or confuse the enemy leader's information, affecting the enemy's ability to make smart or timely decisions.

The U.S. Army has long understood the importance of IO. Units with the ability to collect and analyze information about the battlefield and influence the attitudes and will of the opposition have been in the Army and Army Reserve structures for a long time. The Army Reserve provides many of the units and soldiers that accomplish these missions for the Army such as Civil Affairs, Psychological Operations, Public Affairs, Military Intelligence, and Signal. In fact, almost half the Army's public affairs units are in the USAR and the bulk of the Army's Civil Affairs and Psychological Operations are USAR units.

Recognition of Army Reserve Capabilities

This recognition and new usage of Army Reserve capabilities has brought an ever-increasing number of new requests, requirements, and customers. The list of these customers is growing and includes—the Army's Land Information Warfare Activity (LIWA), Office of the Director of Information Systems for

Command, Control, Communications, and Computers, Army Space Command, Army Research Laboratory (ARL), Army Communications–Electronics Command, the National Ground Intelligence Center, National Security Agency (NSA), Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA), U.S. Space Command (USSPACECOM), and the Joint Reserve Intelligence Program. These commands and agencies are now utilizing USAR units, facilities, and personnel for IO.

The Army recognized these new requirements and has established new organizations to exploit or counter an opponent's ability to use this new technology. The focal point for the Army's IO effort is LIWA. LIWA's mission is to provide IO and Information Warfare (IW) support to land component and separate Army commands, both active and Reserve, and to facilitate planning and execution of IO.

The USAR is building additional capability to reinforce Army IO and LIWA operations. When complete, USAR soldiers will play an important role supporting LIWA's critical mission. The USAR Land Information Warfare Enhancement Center (LIWEC) has been established to directly support and expand LIWA capabilities. Primary elements of the LIWEC include two computer emergency response teams, two information operations vulnerability assessment and detection teams (CERTs), two field support teams, and two operations support sections to LIWA.

The Army Reserve has also created the Reserve Information Operations Structure. Activated to provide support to the Army's computer network defense and IA efforts, the Reserve Information Operations Coordination Center will have five Information Operation Centers (IOCs) containing CERT Support Groups that will identify and respond to viruses and intruders in Army computer networks. Information Infrastructure Defense Assistance Teams will aid in correcting weaknesses in our networks and ensure the execution of corrective actions. The IOCs will also have Technical Research Teams to assist in infrastructure research. Currently, USAR IOCs are forming in the National capital region, Massachusetts, Texas, California, and Pennsylvania.

A Captain from the 315th Tactical Psychological Operations (PYSOPS) Company out of Upland, CA handles crowd control as Humanitarian Aid (HA) items are passed out, August 6, 2000, Koretiste, Kosovo. U.S. Army photo by Sgt. Jason Heisch.

The Challenge of Recruiting for New IO Units and Positions

Recruiting for these new IO units is challenging. Army Reserve soldiers who hold civilian-acquired skills in IT will play a leading role in establishing this new capability. Regardless of what military occupational specialty a soldier has, that soldier can fill one of the growing number of technologically-based IO positions in the USAR. Commuting distance to an IO unit is also not a limitation, as virtual training relationships will allow any qualified soldier to conduct drills and annual training at USAR intelligence support centers or any other suitable facility.

One of the greatest resources in the USAR is the skill soldiers have developed in their civilian training and occupations. The IO units hope to tap into these skills and continue to meet the challenges of warfare in the 21st Century.

Major Williams, USAR is a Military Intelligence Operations Officer, Department of the Army, Office of the Chief of the Army Reserve, Operations Division. He earned his B.A. in History from West Georgia University in 1980 and his M.A. in European History in 1982. He may be reached at greg.williams@ocar.army.pentagon.mil.

Computer Network Defense at the Army Signal Command

by MAJ Mike McNett, USA
and LTC Marc Withers, USA

Imagine an analytical capability and a system that would allow proactive measures to be taken against information threats, rapidly react to new situations, ensure the highest level of network availability to customers, and reduce the vulnerabilities that could be exploited by malicious users. Striving to meet these goals today, as well as fulfilling the DoD's Joint Vision 2020 premise of information superiority, is exactly where the U.S. Army Signal Command's (USASC) Network, Systems and Security Operations Center (ANSSOC) at Fort Huachuca, Arizona is moving in close cooperation with several other organizations. Building upon an impressive base, the efforts underway in the ANSSOC—along with the efforts in USASC's other Theater Network Systems Security Operations Centers—provide the Army with a program that will ensure the highest levels of information assurance (IA) throughout the world, while simultaneously providing high quality service to Army customers.

The ANSSOC is composed of a variety of highly skilled soldiers, civilians, and contractors who are leaders in the field of information technology (IT) and IA. The center provides a variety of network and computer protection services to the Army in the continental United States and worldwide 24x7—managing the Army's Domain Name Service system, providing direct support to key Standard Army Management Information Systems projects, monitoring and protecting the Army's Continental/Contiguous United States (CONUS) information infrastructure above the installation level, managing the Army's dial-in services, and now acting as the public-key infrastructure (PKI) registration authority for private Army Web servers and devices.

The ANSSOC has a day-to-day operational mission of monitoring, managing, and protecting the Army's portion of the CONUS Defense Information Infrastructure (DII). The ANSSOC has successfully teamed with several different organizations to leverage their skills, experience, expertise, and data. Some of these include USASC's other Theater Network, Systems and Security Operation Centers, the Army Computer Emergency Response Team, Defense Information Systems Agency (DISA) and even the Federal Bureau of Investigation (FBI). However, the primary partner of the ANSSOC for IA is the Regional Computer Emergency Response Team-CONUS (RCERT-C).

In addition to close relationships with these organizations, the ANSSOC has ensured success by intertwining network operations with network and systems security and protection. The integration of these two areas has ensured that the ANSSOC is proactive and quick to respond to any threats to the Army infrastructure. This process is enhanced by the co-location of the RCERT-C with the ANSSOC. This allows each organization to leverage off of the other's expertise on a continual basis and has resulted in a partnership that not only ensures a high availability of information to our customers, but has also led to integration of security into all operations (Figure 1).

As part of the Network Security Improvement Program Defense in Depth strategy that is

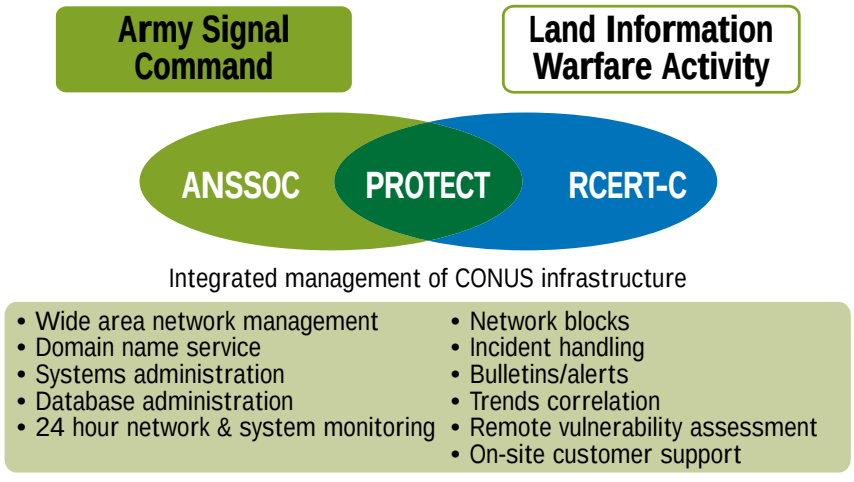


Figure 1. Command and Control Protect Partnership

spearheaded by the Director of Information Systems for Command, Control, Communications, and Computers, the ANSSOC's role in IA is fulfilled primarily above the installation's infrastructure in which lie the demilitarized zones and the installation top level architecture (TLA). The perimeter security of Army installations includes Army security routers (ASR) that route all traffic into and out of each location. These ASRs are centrally managed and monitored at the ANSSOC to ensure both network availability and network protection of the Army's part of the DII at all times.

The next two levels of defense-in-depth are the network-based and host-based intrusion detection systems that the ANSSOC also centrally manages and monitors. This, combined with the ASR status, allows one facility to obtain a common operational view of the entire CONUS DII for the Army's networks and critical servers. These levels are closely tied to and coordinated with the RCERT-C and other agencies.

This defense-in-depth strategy has created a very close relationship between network operations and network and systems security. One example of this close relationship is router log management. Traditionally, routers have been considered network management devices with little attention paid to their role in network security and protection. However, the ASRs located at each installation are dual purpose—they ensure proper routing of traffic and are configured to be "firewall-like" devices. ANSSOC routinely analyzes the logs from these routers to find both network anomalies and potential security events. This results in both highly reliable and secure networks.

In fact, approximately 25 percent of the network security blocks issued are the direct result of router log analysis. These blocks represent malicious activities that occur as low-level attacks, that do not necessarily meet the detection thresholds for the network intrusion detection systems (IDS). If the routers were only viewed with respect to network availability problems, the Army would lose its fight against malicious users since much of this low-level activity would be missed.

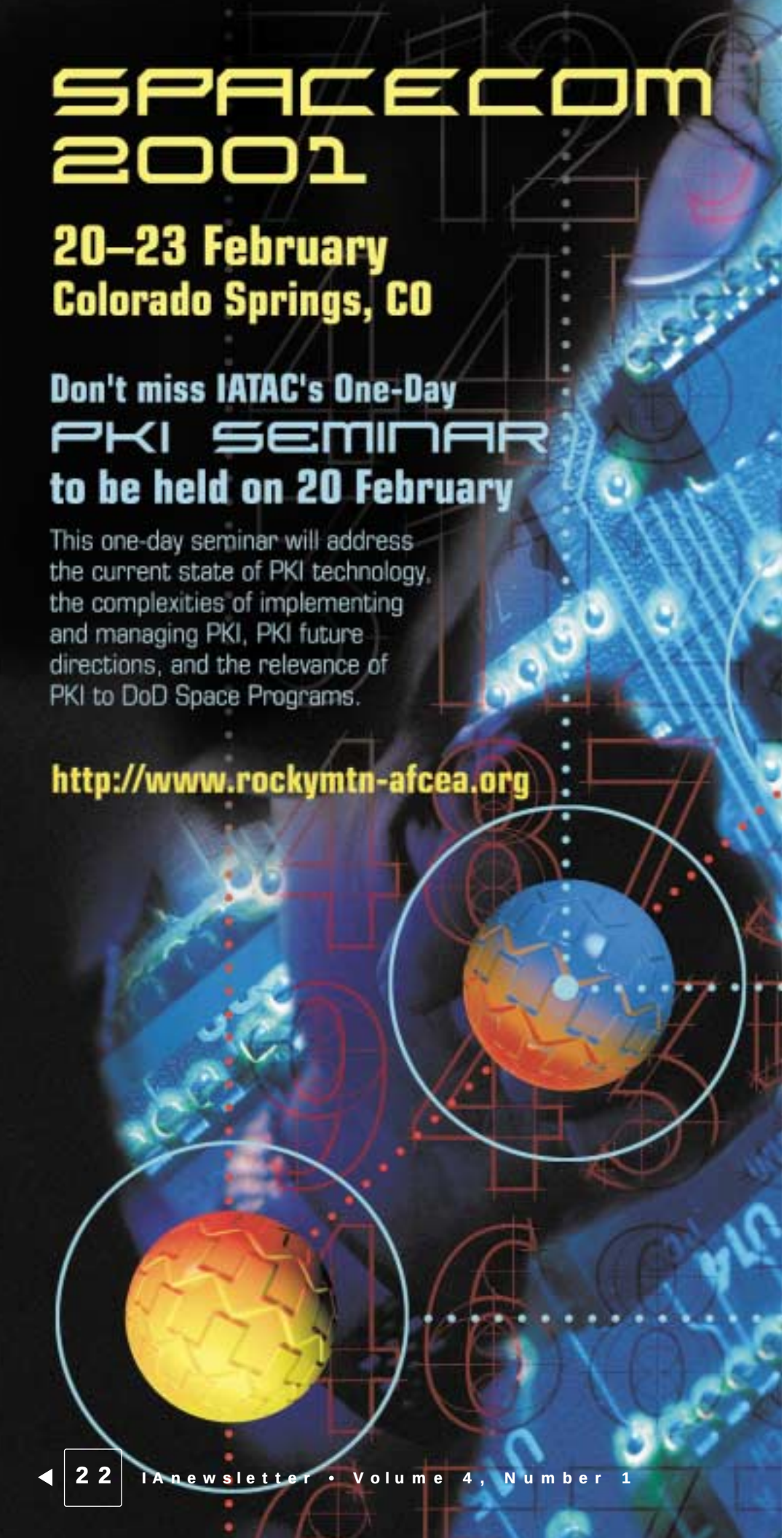
Another example of the synergy resulting from integrated network operations and security occurs during distributed denial of service attacks against Army systems. During such an attack, the network operations portion would see degradation of the network and monitored systems, while the security side of network operations would simply see a large number of events being triggered on the security monitoring devices. By having an integrated network and security operation, the Army obtains a very rapid response to activities such as this by leveraging everyone's skills and abilities.

The structure set up to protect the Army's networks, although successful, is best characterized as a "hasty defense." The Army can now defend itself against frontal attacks (e.g., from "script kiddies"). We can also defend our flanks through existing security mechanisms, policies, procedures, the Information Assurance Vulnerability Assessment (IAVA) process, etc.

However, we are still vulnerable to two types of attacks— the rear battle (backdoors) and the snipers and stealthy individual foot soldiers with lots of camouflage and expertise who are along our perimeter (e.g., sophisticated hackers). They are willing to wait long periods of time to conduct reconnaissance in order to find our exploitable vulnerabilities. To protect against these folks we must expand our defense-in-depth and establish a "deliberate defense"—a more robust top level architecture that has better tools and a more sophisticated architecture able to detect the enemy by looking at all data sources in a coordinated fashion.

This coordination is required because of the multiple sensor devices and information that comes into the ANSSOC—host-based IDS logs for Army critical servers, server logs, firewall logs, network management data, external reports, network-based IDS logs, and router logs. While all of these data sources are valuable when viewed independently, we have found that a great deal of synergy can be gained when we look at this data as a whole. This information would do us little good if we did not have highly qualified and skilled analysts, system administrators, and network managers. However, even the best human cannot correlate all events from all these systems. We need the systems to use their "intelligence" and to help the human.

Event correlation is the technique we are starting to use for this purpose. The ability to correlate between events within one data source is greatly enhanced when you can cross correlate between different types of data sources such as router logs, IDS logs, incident reports, etc. The ANSSOC is currently



correlating data from various data sources to determine when multiple sites are being attacked from the same or multiple sources. This correlation capability has already resulted in an increase in protection across the Army's portion of the DII.

Impressive gains have been made by the ANSSOC (and many other Army organizations) in improving the Army's IA posture and providing security to Army networks. What has been done, however, is just the beginning. We are now moving past the "hasty defense" and making initial changes to implement a "deliberate defense" that takes advantage both of new technologies and new procedures learned over the last few years. The threat continues to evolve, and so must our countermeasures. The ANSSOC is deploying an impressive array of systems to stay at the forefront of the IA battle and integrating network operations with network security. All the Army must strive to do the same.

Major Mike McNett is the director of the Army Network Systems and Security Operation Center for the U.S. Army Signal Command at Fort Huachuca, Ariz. He holds a B.S. in Computer Science from Illinois State University and a M.S. in Computer Science from the University of Illinois. He may be reached at mcnettm@hqasc.army.mil.

LTC Marc Withers is chief of the Network, Systems and Security Management Division for the U.S. Army Signal Command at Fort Huachuca, Ariz. He holds a B.A. in Mathematics and History from the Virginia Military Institute and a M.S. in Computer Science from the Georgia Institute of Technology. He may be reached at withersj@hqasc.army.mil.

FIPS 140-2

The Next Generation

The Cryptographic Module Validation Program

by Mr. Ray Snouffer

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide such services as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for information assurance (IA). Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module could result in insecure products.

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standard FIPS 140-1 (Security Requirements for Cryptographic Modules), and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the Federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are four National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-1 compliance testing; three in the U.S. and one in Canada. By August 2000 over 100 cryptographic modules from more than forty separate vendors were validated through the program. The number of validated modules has nearly doubled each year of the program's existence.

The underlying philosophy of the CMVP is that the user community needs strong independently tested and commercially available cryptographic products. The CMVP must also work with the commercial sector and the cryptographic community to achieve security, interoperability and assurance. Directly associated with this philosophy is CMVP's goal of promoting the use of validated products and providing Federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose products from the CMVP Validated Modules List and can have confidence that the products meet the claimed level of security. The program validates a wide variety of modules including general encryption products, secure radios, virtual private network (VPN) devices, Internet browsers, cryptographic tokens and modules that support public key infrastructure (PKI). Currently, validation services are provided for FIPS 140-1 & 2, the Data Encryption Standard (DES and Triple DES), the Digital Signature Standard, the Secure Hash Standard, and the Skipjack Algorithm.

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1 & 2 and other cryptographic standards. NIST developed the standard and an associated metric (the Derived Test Requirements for FIPS 140-1) to ensure repeatability of tests and equivalency in results across the testing laboratories. The four commercial laboratories provide vendors of cryptographic modules a choice of testing facilities and promotes healthy competition. (Note, there is no limit to the number of testing laboratories, and additional testing laboratories may be added to the program.)

A government and industry working group composed of both users and vendors developed FIPS 140-1. The working group identified 11 areas of security requirements with four increasing levels of security for cryptographic modules. The se-

curity levels allow for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and health data), and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Each security level offers an increase in security over the preceding level. These four security levels allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. This structure also allows great flexibility when specifying or identifying users needs. Modules may meet different levels in the security requirements areas (e.g., a module meets level 2 overall, level 3 physical security with additional level 4 requirements). The Validated Modules List now contains modules representing all four security levels.

FIPS 140-1 &2 define a framework and methodology for NIST's current and future cryptographic standards. The standard provides users with:

- a specification of security features that are required at each of four security levels
- flexibility in choosing security requirements
- a guide to ensuring the cryptographic modules incorporate necessary security features
- the assurance that the modules are compliant with cryptography based standards

The Secretary of Commerce has made FIPS 140-1 mandatory and binding for U.S. Federal agencies and organizations. The standard is specifically applicable when a Federal agency determines that cryptography is necessary for protecting sensitive information. This protection involves situations where products containing a cryptographic module are used when designing, acquiring, and implementing cryptographic-based security systems. FIPS 140-1 is applicable if the module is incorporated in a product, application or functions as a standalone device. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) recently released both an NSTISS Policy and an NSTISS Advisory Memorandum related to FIPS 140-1. NSTISSP 11: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated January 2000 establishes a schedule for implementing evaluated and validated IA-enabled IT products used in national security systems. FIPS 140-1 validation is specified as one of the three accepted methods for evaluation and validation. NSTISSAM INFOSEC/1-00: Advisory Memorandum For the Use of the Federal Information Processing Standards (FIPS) 140-1 Validated Cryptographic Modules in Protecting Unclassified National Security Systems, dated February 2000 further discusses the use of FIPS 140-1 validated modules. The advisory states that, "While NSA [National Security Agency] recommends the acquisition of security products which have been evaluated to determine the robustness of their complete security functionality (preferably against NSA or NIST sponsored Common Criteria (CC) Protection Profiles), products which contain FIPS 140-1 validated encryption modules may be used for the cryptographic protection of unclassified information in national security systems." Additional information on these two documents may be obtained from the NSTISSC Secretariat at NSA.

From the beginning, the CMVP has been dynamic—constantly reexamining the underlying standard, test methodology, reporting structure, and associated documentation. In addition, questions from the vendor and user communities have provided valuable input and an implementation perspective. NIST and CSE have continually kept pace with new security methods, changes in technology, and required interpretations of the standard by issuing official Implementation Guidance and Policy for FIPS 140-1 and associated Derived Test Requirements. The Implementation Guidance covers program policy, technical questions, and general guidance needed for module validation.

In addition to constant reexamination, the standard is officially reexamined and reaffirmed every five years beginning in the Fall of 1998.

For more information on FIPS 140-2 visit our Web site at http://csrc.nist.gov/cryptval.

Mr. Snouffer earned his B.A. in mathematics from Western Maryland College in 1986. Since January 1997, he has served as the Program Manager for the Cryptographic Module Validation Program and now also serves as the supervisor of the Cryptographic Security Testing Program Area of NIST's Computer Security Division. He may be reached by E-mail at ray.snouffer @nist.gov.

IATAC chat

by Robert J. Lamb, IATAC Director

Robert P. Thompson

During the past quarter IATAC has undergone a change in directorship. Bob Thompson has assumed new responsibilities overseeing the 80+ IATAC Technical Area Tasks (TATs) currently in operation and establishing the first IATAC Satellite Office in Tampa, Florida. His additional responsibilities will include representing SURVIAC and HSIAC in providing scientific and technical support to the warfighter.

I'd like to publicly thank Bob for his outstanding leadership as the Director over the past two and a half years. He has been the guiding force in building IATAC from its very foundation as a "virtual Information Analysis Center (IAC)" to its position today as a major contributor to the IA community.

Among his many contributions are this publication. It has become a first class forum for presenting topics of interest to the entire IA community—from the foxhole to OSD. Similarly, our many Critical Review Technology Assessments (CR/TA) and State of the Art Reports (SOAR) have proven timely and well received by IA professionals and leaders, system administrators and commanders alike.

One of Bob's many initiatives has been the IATAC Satellite Office and it is with great pleasure that IATAC announces the opening of its first Satellite Office in Tampa, Florida on 15 November 2000. Working closely with the DISA Field Office, this first IATAC Satellite Office will support Special Operations Command (SOCOM) and Central Command (CENTCOM). It will provide liaison support for IATAC and IAC program initiatives and is an extension of IATAC core operations. As such, the Satellite Office will serve as the initial point-of-contact for locally generated inquiries (technical and bibliographic), maintain and distribute IATAC and IAC products, promote current awareness activities, and provide management and oversight of local IATAC TAT execution.

Steering Committee

This past June, IATAC held its annual Steering Committee Meeting. The Steering Committee consists of IA professionals from across the community and is chartered to review IATAC activities and provide advice and guidance on future IATAC operations. The Steering Committee identified four critical subject areas for this year's reports.

The Malicious Code SOAR will update the previous SOAR of the same name, providing a background on the nature of the malicious software problem and the threat that it poses to DoD systems. The goal for this report is to address the problem of malicious code detection from a pragmatic perspective.

The Information Assurance (IA) Modeling and Simulation (M&S) SOAR (jointly written with MSIAC) will provide a full representation of IA M&S tools supporting today's warfighter to meet the challenges described in Joint Vision 2020 (JV2020). This includes tools used for budgetary tradeoff analyses (availability of proper systems), systems acquisition design analyses (designed to meet their intended requirements), and training and exercise support (so the warfighter knows how to employ them properly).

The Configuration Management Compliance CR/TA will examine compliance with Information Assurance Vulnerability Alerts (IAVA) and the tools available for ensuring compliance.

The final CR/TA will summarize Applied IA Development Initiatives in DoD Labs and examine those efforts, which are either being conducted or funded by DoD.

SPACECOM PKI Seminar

Finally I would like to mention that IATAC will be sponsoring a one day Public Key Infrastructure (PKI) seminar on 20 February 2001 in conjunction with and preceding the SPACECOM 2001 Conference to be held in Colorado Springs, Colorado 20–23 February 2001. This one-day seminar will address the current state of PKI technology, the complexities of implementing and managing PKI, future directions, and the relevance of PKI to DoD Space Programs.

For more information on this seminar or IATAC's upcoming CR/TAs and SOARs, contact IATAC at 703.289.5454 or via E-mail at iatac@dtic.mil.

order form

IMPORTANT NOTE: All IATAC Products 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/regprocess.html.

Name _____ **DTIC User Code** _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

LIMITED DISTRIBUTION

IA Collection Acquisitions CD-ROM

❑ June 2000

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics ❑ Computer Forensics* ❑ Defense in Depth ❑ Data Mining
❑ IA Metrics ❑ Modeling & Simulation*

IA Tools Report

❑ Firewalls (2nd Ed.) ❑ Intrusion Detection (2nd Ed.) ❑ Vulnerability Analysis (2nd Ed.)

State-of-the-Art Reports (SOARs)

❑ Data Embedding for Information Assurance ❑ IO/IA Visualization Technologies

❑ Malicious Code Detection* [❑ TOP SECRET ❑ SECRET] _____

Security POC _____ Security Phone

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

UNLIMITED DISTRIBUTION

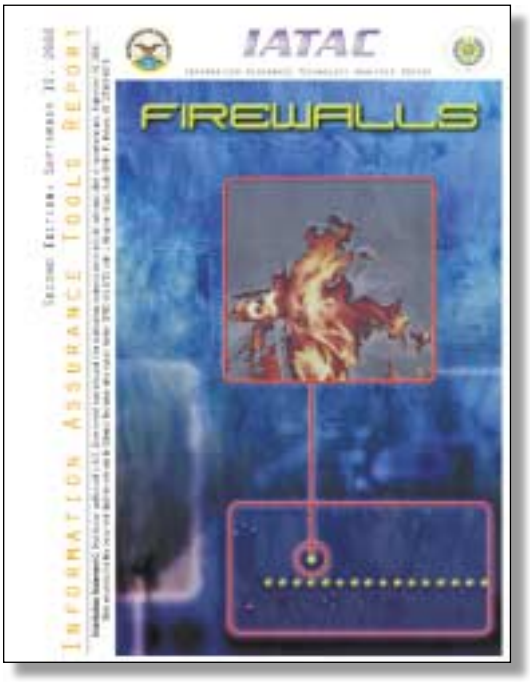
Newsletters *(Limited number of back issues available)*

❑ Vol. 1, No. 1 ❑ Vol. 1, No. 2 ❑ Vol. 1, No. 3
❑ Vol. 2, No. 1 ❑ Vol. 2, No. 2 (soft copy only) ❑ Vol. 2, No. 3 ❑ Vol. 2, No. 4
❑ Vol. 3, No. 1 ❑ Vol. 3, No. 2 ❑ Vol. 3, No. 3 ❑ Vol. 3, No. 4
❑ Vol. 4, No. 1

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

_____

Once completed, fax to IATAC at 703.289.5467



Firewalls 2nd Edition

Responding to a need to provide information to customers so they can make informed decisions about how to safeguard their Internet transactions, the Firewalls Tool Report contains descriptions of 47 tools. This newly updated report provides an index of the firewall tools, which are also described in the IATAC Firewalls Tools Database. For this report a firewall is a component or set of components that restricts access between a protected network and an unprotected network. It summarizes pertinent information, providing users with a brief description of available firewall tools and contact information. The tools are classified by the following categories: Internet Protocol (IP) packet filtering, application gateways, packet inspection, hybrid firewalls, and virtual private networks. The written descriptions highlight the capabilities and features of each firewall product. New in this edition of the report, are sources of product evaluations. As a living document, this report will be updated periodically.

IO/IA Visualization Technologies State-of-the-Art Report (SOAR)

This report provides a synopsis of the information visualization industry, the industry's associated technologies, and visualization methodologies. It is written for a broad audience, principally for those unfamiliar with this technology, new to the industry, or seeking visualization capabilities for the first time. This report is written for system users. Visualization is, by nature, user-centric. Visualization technologies, for example, allow users to interact with information systems. Therefore, users must first understand what visualization is, what its capabilities and restrictions are, and what ideas factor into its use.

This SOAR should help readers decide whether visualization is appropriate to their needs, determine what types of visualization technologies are available and relevant, and formulate possible strategies for implementing a visualization solution.

Biometrics

Fingerprint Identification Systems

Focuses on fingerprint biometric systems used in the verification mode. Such systems, often used to control physical access to secure areas, also allow system administrators access control to computer resources and applications. Information provided in this document is of value to anyone desiring to learn about biometric systems. The contents are primarily intended to assist individuals responsible for effectively integrating fingerprint identification products into their network environments to support the existing security policies of their respective organizations.

Calendar

January 23—25

WEST 2001
San Diego Marriott
San Diego, CA
http://www.west2001.org/travel.htm
COME VISIT US AT BOOTH #1250

25

Information Assurance Technical Framework Forum
Maritime Institute of Technology and Graduate Studies
Linthicum, Maryland
POC: Mr. John Niemczuk
410.684.6246
niemczuk_john@bah.com
http://www.iatf.net

February 6—8

5th Annual Information Assurance (IA) Workshop
Jointly sponsored by the DISA, USSPACECOM and NSA
Sheraton Norfolk (Waterside) Hotel, Norfolk, Virginia.
"Information Assurance—Enabling Joint Vision 2020"
http://iase.disa.mil

20—23

SPACECOM 2000—A SpaceCOMM Odyssey
Sheraton Hotel, Colorado Springs, Colorado
http://www.rockymtn-afcea.org/2001/2001home.htm
IATAC will be presenting a PKI Seminar on the 20th!
VISIT US AT BOOTH #69

March 13—14

TechNet Tampa 2001
"Preparing for and Responding to Asymmetric Threats"
Tampa Convention Center
http://www.afcea.org/tampa/
COME VISIT US AT BOOTH #312

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