PUBLISHED BY THE INTERAGENCY OPSEC SUPPORT STAFF

THE OPSEC INDICATOR

Volume XI

Winter 2001

"Meeting The Challenges of a Changing World"

ATF Establishes Law Enforcement Network to Focus on OPSEC

by Lynne M. Yates
IOSS Staff

On September 27, the Bureau of Alcohol, Tobacco and Firearms (ATF) hosted its first gathering of a network of law enforcement professionals interested in learning more about operations security (OPSEC) at its headquarters in Washington, D.C.

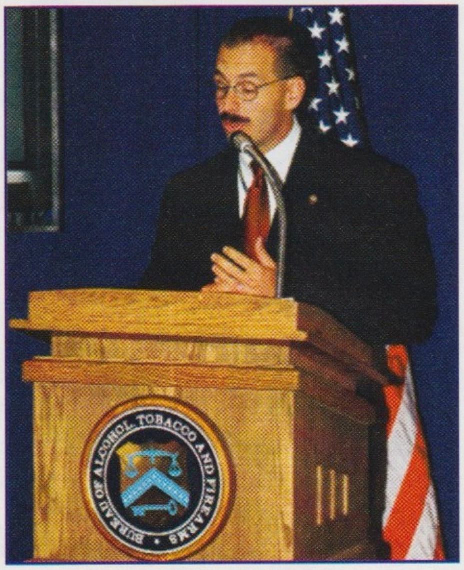
In an effort to further the practice of operations security, the ATF will be sponsoring meetings of this law enforcement network quarterly for the members to share OPSEC information and discuss success stories or problems encountered in a roundtable forum.

Representation

Representatives from the ATF, the U.S. Mint Police, the U.S. Secret Service, the U.S. Customs Service, the Department of State, The Department of Immigration and Naturalization, the General Services Administration (Federal Protective Service), the Federal Emergency Management Agency, the Federal Aviation Administration, the U.S. Capitol Police, the Postal Inspection Service, and the Internal Revenue Service were in attendance.

All of these organizations have clearly defined law enforcement missions and the representatives in attendance were very interested in acquiring more information on how the effective application of OPSEC could enhance their overall security posture.

Mr. Tom Mauriello, Director of the the Interagency OPSEC Support Staff (IOSS) and Mr. Pat Geary, the president of the OPSEC Professionals Society (OPS) were the featured speakers.



Mr. Madison P. Townley, Chief, Operations Security, ATF

New Focus

The session began with a welcome from Mr. Mark Logan, the Assistant Director, Liaison and Public Information for the ATF. Participants then received an introductory briefing from Mr. Madison P. Townley, Chief, Operations Security, for the ATF.

Townley began by describing how the ATF recently and dramatically shifted its OPSEC focus. Townley recalled that in 1999, his supervisor told him that OPSEC needed to become an integral part of ATF field operations. This would necessitate direct OPSEC support to law enforcement operations throughout the country.

As a result of the greater emphasis on OPSEC, Townley was given a bigger budget and a larger staff and his office began taking OPSEC "on the road" to support agents actively involved in ATF operations. This new OPSEC focus resulted in many success stories—missions were completed, arrests were made (thanks to the element of surprise being maintained), and no physical harm came to anyone involved.

Townley stated, "With this group here today, we hope to facilitate new ideas, techniques and trends and see

Inside This Issue:

what's going on out there. We hope to roll up our sleeves and really come up with an OPSEC product. It may incorporate how we share information, how we apply different techniques, or how we share intelligence."

He continued, "We realized early on that information sharing is critical. When we assist an agent in an undercover operation, if we don't have good intelligence to start with, our program is weak. What *we* do is help the agents identify the critical information and apply the process."

"That's what our current goal is, and that's what we hope to build on with this group, to actually share the knowledge that is out there and make it available to those who need it."

A United Front

Townley concluded, "The idea for this forum sprang from a recent joint task force operation that the ATF conducted with the Secret Service and the FBI.

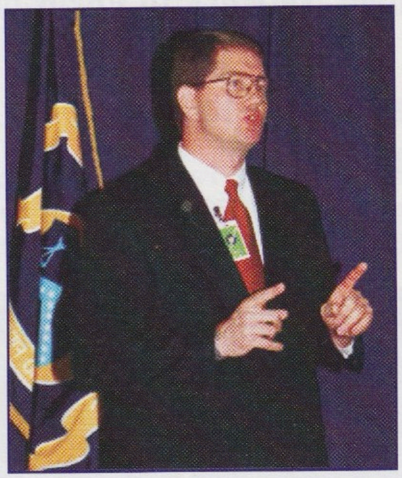
We all came to realize that when we hit the ground on these operations we sometimes spend two or three days discussing what everyone is going to do. If we were already united, we could at least eliminate that aspect of it...we'd know what was expected, we'd know how to do it, and we could just *go*."

After Townley's presentation, participants from the various agencies introduced themselves to the group and related how OPSEC could be used in their operations. The participants were uniformly enthusiastic about OPSEC and their involvement in the group.

The IOSS Connection

Tom Mauriello, Director of the Interagency OPSEC Support Staff (IOSS) was the first guest speaker. Mauriello expressed his gratitude to the ATF for gathering all of the law enforcement professionals together for the forum. He praised the strides that the ATF's OPSEC program has made and stressed the need for OPSEC in law enforcement and related disciplines.

Mauriello stated that, as someone with a security, law enforcement, and counterintelligence background, he has come to believe that, "in the Information Age, we cannot survive without the OPSEC process—OPSEC is not a security discipline, it is an analytic process. Unfortunately, arguing about semantics has caused some people to shy away from OPSEC and we cannot afford to let this happen."



Mr. Pat Geary
President, OPSEC Professionals Society

Mauriello also remarked that "OPSEC was ahead of its time." He presented a brief history of the formal recognition of OPSEC beginning with the "Purple Dragon" operation in the Viet Nam war. He outlined the provisions of National Security Decision Directive (NSDD) 298 which proclaimed that every organization with a national security mission *must* have a formal OPSEC program.

Mauriello elaborated on how the IOSS has been providing training, products, surveys, and other services to all those interested in establishing formal OPSEC programs since 1988. He offered the services of the IOSS to all of the attendees.

Mauriello concluded his presentation by previewing the latest IOSS video, (coincidentally produced by the IOSS for the law enforcement community). He explained that the video was designed to demonstrate to the law enforcement community exactly how OPSEC fits into its day-to-day operations.

Each participant received a copy of the video, entitled ***"Applying OPSEC to Criminal Investigations"*** for use in their parent organizations.

OPS

Mr. Pat Geary, the newly elected President of the OPSEC Professionals Society was the final speaker of the morning. Geary explained the role of the OPS and outlined the many benefits of joining that unique society.

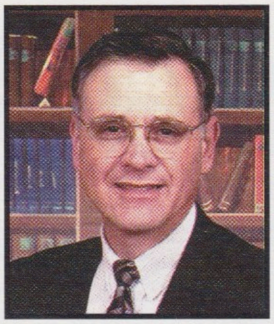
Geary stated that the OPS was founded in 1990 in response to NSDD 298. The goal of the OPS is "to enhance the professionalism and competence of our profession...the society was created as a vehicle to that end." He added, "It is the analytical process of OPSEC that the OPS is trying to enhance."

In Geary's opinion, the main focus of OPSEC in law enforcement is to increase the element of surprise.

Geary provided applications for membership in the OPS. He concluded by emphasizing how valuable the OPS can be in networking with other OPSEC professionals in Federal, state and local agencies. Members of the society are a cross-section of security, counterintelligence, law enforcement and other related disciplines that use OPSEC.♦

The ATF will be conducting the second law enforcement OPSEC working group on February 8 at their headquarters in Washington, D.C. All Federal law enforcement organizations are encouraged to get involved. For further information, call (202) 927-1020.

Director's Message



OPSEC Success in the New Millennium

Let me begin my first message of the new year by wishing you all the best as you enter the "real" new millennium. I hope that you and your families had a wonderful holiday season and that you are refreshed and ready to meet a new year full of OPSEC challenges.

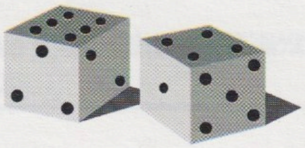
It occurs to me that we in the protection business are not considered important unless someone dies, is injured, or national security has been critically threatened. Therefore, we are always in a reactive mode, and not taken seriously until publicity overpowers the ability to ignore us. So what can we do to change this? How can we in the OPSEC community demonstrate the significance of the operations security process?

One thing we must do is tell the stories that illuminate our worth. We must be open to letting others know how OPSEC made a difference, saved a life, identified a vulnerability, reduced cost, or just made sense in this complex world of ours. Many are unwilling to invest in a supportive function like OPSEC unless we can prove its value and its direct advantage to the mission. We have convinced ourselves that we make a difference, so why can't we convince our senior leadership of the same? The fact is that a presidential directive and regulatory policy requiring OPSEC has not been enough. So we must try a different strategy.

This has been tried before, but I want to try again. The IOSS wants to collect OPSEC success stories. The purpose would be to feature them in a briefing document for all to use to convince senior leadership of OPSEC's role within the foundation of every organization. These stories must be unclassified and obviously must not expose any critical information. We need specifics about the OPSEC programs and tools used by your organizations.

*Remember, we are looking for organized OPSEC applications that provided the necessary protection services that demonstrate evidence of value-added activities. Send them to me directly. I promise you that we will share them in a manner that will change people's minds and convince them to seek our services. Visit **www.ioss.gov** and click on "OPSEC Success Stories." You will find a form that you can download and fax directly to me at the IOSS on 301-982-2913.*

In closing, I would also like to extend my condolences to the family of George Jelen. Mr. Jelen, a former NSA OPSEC Program Director, passed away this past fall. In his honor, we have named the national OPSEC literature award, "The George F. Jelen Literature Achievement Award." See the story on page 13 about George's accomplishments in the OPSEC community while leading the development of the IOSS in the early 1990's.



Tommy

Upcoming Training Courses and Symposia

The IOSS offers numerous training classes to support OPSEC. Several minor changes have been implemented in our curriculum for Fiscal Year 2001. Our OPSEC Fundamentals Course (OP-300) is now a one-day course designed to teach the basics of what OPSEC is and is not. The OPSEC Practitioner's Course (OP-380) is a 5-day course covering OP-300 objectives and implementation of OPSEC tools, skills and processes. Our OPSEC Program Manager's Course (OP-390) is now a 3 1/2–day course (it was previously 4 days). There is no tuition fee for IOSS courses and all courses can be tailored to organizational requirements and presented at a location of your choice by an IOSS mobile training team (MTT).

Organizations requesting MTT support are asked to pay travel and per diem for IOSS instructors. Contact the IOSS training team at (301) 982-0323 to arrange MTT classes. Our schedule of training offered at the National Cryptologic School and IOSS headquarters is provided below. In addition, training is routinely offered in conjunction with our Regional Threat Symposium, Regional OPSEC Symposium and our National OPSEC Conference and Exhibition, also listed on the training schedule.

Visit the IOSS web page, ***www.ioss.gov,*** for updates on training, specific course descriptions, training opportunities at IOSS events, and IOSS products. Registration for IOSS courses is easy, and instructions for registering are provided on our web page. Simply click on the "Calendar of Events" button — registration information is provided at the bottom of that web page.♦

6-7 February—Regional Threat Symposium—Las Vegas, NV

12 February—OP-300, OPSEC Fundamentals Course—NCS

5-8 March—Regional OPSEC Symposium—Norfolk, VA

26-30 March—OP-380, OPSEC Practitioner's Course—NCS

2-5 April—OP-390, OPSEC Program Manager's Course—IOSS

24 April—OP-300, OPSEC Fundamentals Course—NCS

7-11 May—OP-380, OPSEC Practitioner's Course—NCS

11-15 June—National OPSEC Conference & Exhibition—Tampa, FL

16-20 July—OP-380, OPSEC Practitioner's Course—NCS

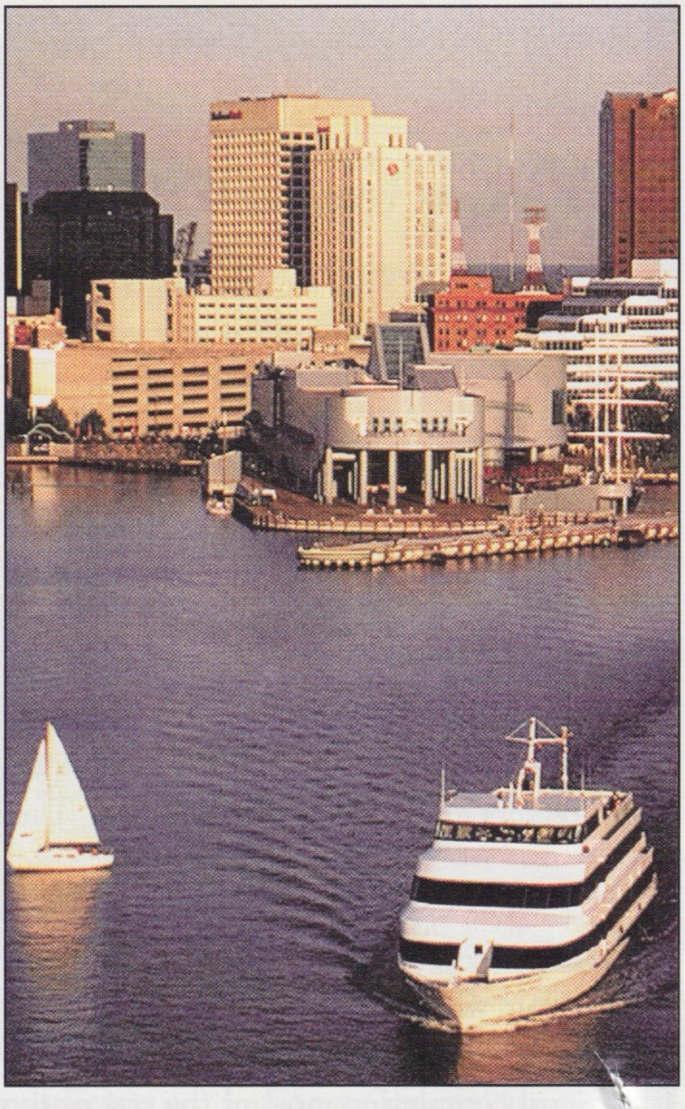
23-26 July—OP-390, OPSEC Program Manager's Course—IOSS

8 August—OP-300, OPSEC Fundamentals Course—NCS

21-23 August—Web Content Vulnerabilities Seminar—IOSS

10-14 September—OP-380, OPSEC Practitioner's Course—NCS

REGIONAL OPSEC SYMPOSIUM
NORFOLK, VIRGINIA
MARCH 5-8, 2001



Training

The following all-day courses will be offered on Tuesday, March 6. Participants attending on Tuesday will be asked to pre-register for one of these courses:

OP-300, OPSEC Fundamentals is accredited by the National Cryptologic School (NCS), and is designed to familiarize students with the 5-step OPSEC process. Students receive 8 credit hours.

Threat Research provides an overview of information resources available to the OPSEC analyst, and a suggested approach to gathering all information into a cohesive, accurate assessment of the intelligence threat to an operation or activity. This is an 8-hour course. This seminar will require a U.S. SECRET clearance.

Computer Network Defense provides the OPSEC practitioner with an overview of the fundamentals of computer network protection. It addresses basic definitions, principles and best practices, and how network vulnerabilities can have an impact on OPSEC implementation.

Clearances

A U.S. SECRET clearance is required for all sessions on Thursday, March 8. Instructions for providing clearance certification are at ***www.iaevents.com***. Please contact McNeil Technologies at 410-553-6465 or by e-mail at kahenthorn@mcneiltechmd.com to pass clearances by fax or mail. Verification that clearances have been received is also available at this e-mail address.

Register on-line!

Schedules, fees, and lodging information for both events is available at ***www.iaevents.com.*** On-line registration is available for both events at this site if you use a credit card to pay fees.

For an updated agenda of additional speakers and topics visit *www.ioss.gov*. To register by mail or fax, contact McNeil Technologies at 410-553-6465.

It's A New Year at OPS!

The OPSEC Professionals Society (OPS) has begun a new year and we want you to be a part of it.

We have a number of events and activities coming up including "OPS - 2001" to be held in Las Vegas; a joint OPS/ASIS event to be held in the Washington, DC area; and of course, the National OPSEC Conference to be held in Tampa with our IOSS partners.

Check out the details for these and some of our other upcoming activities on our website: www.opsec.org. We also have a new slate of National Officers, a new Board of Directors and lots of new members. The only missing part is you! Join us.

The OPS Board of Directors has adopted 10 new goals for this year in the hope of advancing our profession. One of our most important goals is to forge a closer relationship with the IOSS. Thanks in part to IOSS Director Tom Mauriello, we are well on our way toward achieving that goal. We have already made substantial progress toward completing most of the rest of those goals.

We are looking forward to advancing our profession with our IOSS partners and we hope you will be there with us. For information on 9 great benefits of joining OPS as well as details on our events and activities, be sure to check out the OPS website.

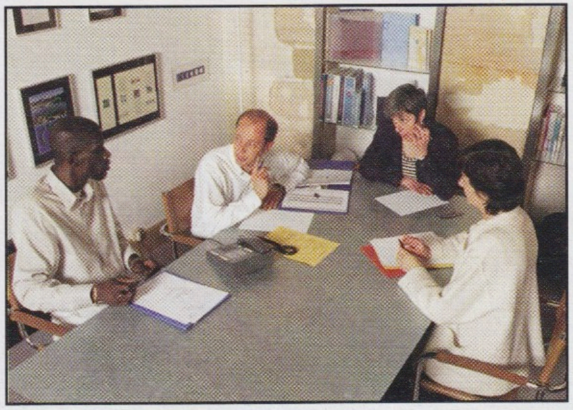
Patrick Geary
9th National President
OPSEC Professionals Society

Program Development Team Pilots New Working Group

by John Glorioso
PDT Manager

The IOSS Program Development Team (PDT) of the Interagency OPSEC Support Staff (IOSS) will be initiating a working group directed toward supporting the OPSEC manager. The working group will consist of individuals assigned to manage an OPSEC program for their organization.

The idea for this working group was an outgrowth of a discussion between OPSEC managers attending the last OP- 390 course at the IOSS and the course facillitators.



It was agreed that a forum was needed for managers to meet and discuss various organizational issues impacting the use of OPSEC within their organizations.

Working Group Goals

It was projected that the working group would meet periodically at the IOSS or at the worksites of the participants. The meetings would concentrate on relevant issues concerning the implementation of successful OPSEC programs.

During the meetings, members will discuss their programs and share both program development problems and program successes.

By candidly discussing what works and what doesn't, group members should obtain some insight into what might be missing from their respective programs.

The PDT will facilitate the initial meeting but will call upon participants to form their own committee, set group goals, and establish those things needed to ensure a successful working group. The PDT's role will be to assist and support the group.

The First Step

The PDT has already taken the first step in establishing the program. Letters were sent to individuals who have attended the OP-390 and work in Baltimore, MD, Washington, D.C., or the surrounding areas. The initial letters solicited any individuals interested in forming the group who were also willing to undertake an active and continuing role in its existence. Some participants may be asked to accept a management role in the group or to provide assistance when necessary.

The OPSEC Manager's Working Group will belong to the OPSEC managers and coordinators—the PDT will merely provide support and guidance.

Composition of the Working Group

The OPSEC Manager's Working Group is designed to bring together individuals responsible for promoting and conducting an OPSEC program either in the private sector or in government.

Although the PDT initially forwarded letters only to those colleagues who attended an OP-390 at the IOSS or at a nearby site, participation is open to anyone in this category.

Long Distance Participants

For those of you assigned as OPSEC managers who are located at distances too far away to travel to the OPSEC Manager's Working Group meetings, you may be able to communicate your OPSEC program concerns by teleconference, phone, or e-mail.

A website will be established on the IOSS Homepage, designed to keep OPSEC managers informed of the progress of the working group.

It is important to note once again that OP-390 attendance is ***not*** a prerequisite for membership in the OPSEC Working Group. If you have been unable to attend the course, you may belong to the group if you are an OPSEC manager or coordinator or have oversight of an organization's OPSEC program.

How Do I Sign Up?

If you are interested in participating in the OPSEC Manager's Working Group, either by attending the meetings or communicating your concerns electronically, call or e-mail Sandy Weizer at 301-982-0323 or send an e-mail to s.weizer@radium.ncsc.mil or John Glorioso at 301-507-6232 or e-mail to j.glorio@radium.ncsc.mil.

The IOSS/PDT is interested in providing any assistance necessary in establishing, revitalizing or continuing active and productive OPSEC programs.♦

The IOSS in partnership with OPS invites you to the 12th Annual National OPSEC Conference and Exhibition

NATIONAL OPSEC CONFERENCE AND EXHIBITION

Westin Innisbrook Resort
June 11 - 15, 2001
Tampa, Florida

To register online visit www.iaevents.com

Schedule of Events

Sunday, June 10
Registration
Monday, June 11
Registration
Pre-Conference Seminars
Tuesday, June 12
Registration
National Awards Luncheon
Unclassified Sessions
OPS Annual Meeting
Wednesday, June 13
Registration
Sessions (Classified and Unclassified)
Exhibits Open
Thursday, June 14
Registration
Sessions (Classified and Unclassified)
Exhibits Open
Friday, June 15
Post-Conference Seminars and Workshops

About the Conference

The conference is designed to provide training and networking opportunities for professionals in management, security, intelligence, infrastructure protection, counterintelligence, military operations, and related fields.

Exhibits

The exhibit area continues to offer a wide array of industry and government exhibitors. The $850 fee includes pipe and drape, an ID sign, one table, two chairs, two exhibitor staff badges, lunch on Wednesday and Thursday, and one conference pass. Contact McNeil Technologies, (410) 553-9275, for more information.

Session Abstracts

Visit the IOSS web page at ***www.ioss.gov*** for a draft schedule and session abstracts.

Pre-conference Seminars – June 11

Five unclassified pre-conference seminars will be available at no additional charge. The Fundamentals of OPSEC course, OP-300, is accredited by the National Cryptologic School and students will receive credit.

Technical Sessions and Workshops – June 12-14

Technical Sessions are briefings on a variety of subjects designed to provide new information and insight for participants from novice to expert. Workshops will be three-hour sessions designed to provide participants with a skill or ideas shared by other professionals to enhance their professional skills and programs.

Workshop leaders are experienced practitioners. A special four-hour accredited seminar will be offered with four credit hours available from the National Cryptologic School.

Classified Sessions

All classified briefings on June 12 and 13, and classified seminars on June 15 require a U.S. SECRET clearance to attend.

Post-conference Seminars and Workshops – June 15

Three post-conference seminars and two workshops will be offered at no additional charge. Two of the seminars are classified U.S. SECRET; all other Friday sessions are unclassified.

OPSEC Professionals Society Annual Membership Meeting

OPS will hold its annual reception and membership meeting on Tuesday evening, June 12, 2001. While only members are permitted to vote during the meeting, all conference participants, spouses, and friends are invited. Contact OPS at (301) 840-6770, or visit the website at ***www.opsec.org*** for more information on the meeting agenda, or to pre-register.

Accommodations

The Westin Innisbrook Resort (36750 US Highway 19 North, Palm Harbor, FL) is the official headquarters for the conference. The conference rate for all participants is $120/night. This rate is guaranteed until May 11, 2000; make your reservations early to meet the deadline. Call 1-800-228-3000 and be sure to ask for the conference group rate.

Conference Fee

The 2001 fee is $250.

Registration and Security

Registration or security clearance verification questions should be directed to McNeil Technologies at 410-553-6465. Clearances can also be verified via email to kahenthorn@mcneiltech-md.com.

Cancellation Policy

Only written cancellations accepted. Full refund prior to April 7; prior to May 15, receive 50%; no refunds after May 15. Substitutions are permitted at any time. You may fax a written request for refund to McNeil Technologies at (410) 553-9275.

Registration is available on line at ***www.iaevents.com***. Contact McNeil Technologies at (410) 553-6465 to receive registration materials by fax or mail.

2001 National OPSEC Awards Luncheon

The 2001 National OPSEC Awards will be presented at a luncheon on Tuesday. For more information on the Awards program call the IOSS at (301) 982-0323.♦

Anyone Seen A Truck?

The Case of the Missing SIGABA Machine

by Patrick D. Weadon
NSA Historian

The last 30 years have brought to light a number of intriguing stories regarding the Allies' prowess in breaking the diplomatic and operational codes of the Axis powers during World War II.

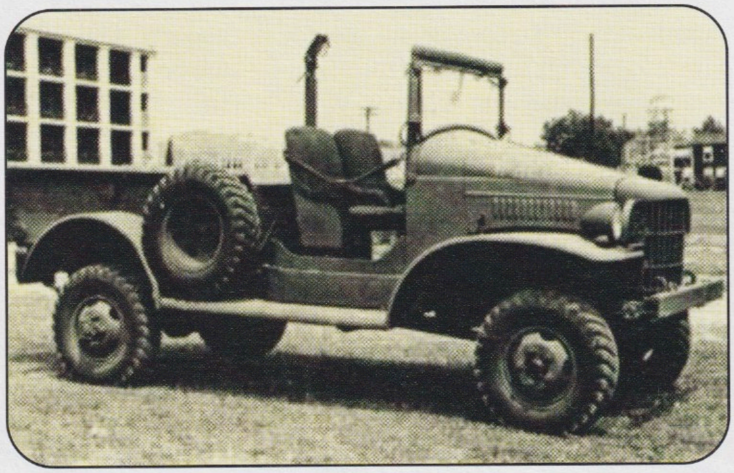
These activities provided an immense advantage to the war effort and afforded senior level commanders in the European and Pacific Theaters the ability to know the who, what, when, where, and how of enemy intentions.

When historians and pundits discuss World War II intelligence successes, they usually focus on the codebreaking side of the equation. They sometimes forget that the protection of our own critical information was also a major factor in subduing the Third Reich and Dai Nippon.

Many have heard of the breaking of the German Enigma code machine and the important cryptologic work that led to the destruction of the Japanese fleet at Midway, but few ever talk about the equally impressive story of the SIGABA device which allowed the Allies to protect their own critical information from being exploited.

SIGABA

SIGABA was the brain child of Mr. William Friedman, "The Father of American Cryptology." Like the German Enigma device, it depended on a series of rotors to ensure its security. Unlike the Enigma, however, it proved to be flawless in its efforts to provide a safe and secure way to relay top-level critical information.



The SIGABA program, like its codebreaking counterparts, was a combination of intellectual brilliance and "good old American know-how." Its inventors did their job well—the German codebreakers trying to decipher the machine's codes became so frustrated that they eventually gave up. Over a half-century later, there still is not one recorded instance when the Axis was able to crack the device.

The Perfect Situation

By late 1944, Allied codemakers and codebreakers had a perfect situation. On the one hand, they had the capability to snatch and decipher enemy communications, almost at will. On the other hand, thanks to the SIGABA, they could communicate with the knowledge that their critical information was secure.

At first glance, it would appear that, in terms of intelligence work, the Allies were pitching a perfect game. However, as cryptologic historian David Kahn relates in Chapter 15 of his book **"The Codebreakers,"** the Allies came perilously close to losing one of their most precious resources, the SIGABA.

This potentially cataclysmic event was not due to faulty engineering or mathematical oversight, but rather to the one vulnerability that is perhaps the most difficult to counter—human nature.

Countermeasures

Due to the importance of the impenetrable SIGABA device in protecting critical information, commanders demanded a series of security measures be implemented to protect it. Kahn notes that many of the units close to the front lines chose to move the SIGABA to the rear on a daily basis.

Another measure was that the device, and the various implements required to operate it, had to be stored in three separate heavy-duty safes; one for the device itself, one for the rotors (which were the key to the machine's security), and one for the key lists containing the rotor settings to be used on a particular day.

These machines were guarded constantly. All of these countermeasures worked quite effectively—that is, until the night of February 3, 1945.

Intermezzo

On that fateful evening, two sergeants of the 28th Division were entrusted with transporting the SIGABA by truck to a new location near Colmar, France.

Seeking to find some relief from the strain of battle, the two intrepid warriors made a command decision to take an unscheduled break at what is sometimes referred to as a "cat house." After their brief respite, our heroes emerged to discover that the truck containing the three safes had disappeared!

Later that day, Allied agents found the trailer that had been attached to the truck on the side of a nearby road, but there was no sign of the truck or the safes.

The SIGABA Machine

Terror and Dread

As one would expect, General Eisenhower and the senior commanders were filled with a sense of terror and dread. Colmar was close enough to the front lines that it was entirely possible that the Germans had stolen the device. If this were the case, it would be catastrophic to the Allied war effort.

On the positive side, a risk assessment determined that future communications could remain secure because the rotors and the keys could be changed to ensure the safety of future transmissions of critical information.

A huge vulnerability remained. If the Germans were in possession of the device and the keys, they had the capability of reading past messages – those snatched from the ether by the Third Reich but previously unreadable. If the old intercepts could now be read, the Germans would be able to discern past Allied logistical trails, operation plans and intelligence capabilities.

In short, the loss of the device could cost thousands of lives and needlessly prolong an already horrible conflict.

The Search

Supreme Headquarters made it an immediate priority to find the missing SIGABA and get it back. General Eisenhower assigned his chief counterintelligence officer, Colonel David G. Erskine to the job. He instructed him to find the missing items at all cost.

A special squad of American and French agents was formed to recapture the device. The squad had an inauspicious debut. Shortly after its formation, two of ***their*** jeeps were stolen, prompting Ike to appoint a major general, Fay B. Pickett, to oversee the operation.

For weeks, every conceivable possibility was checked out. Allied spies in Switzerland and the surrounding area were queried to determine if they had any information indicating that the Germans were celebrating their good fortune; nothing turned up.

Even the possibility that the French allies may have pinched the device was explored. This theory was also proven to be invalid.

A Lucky Break

Finally, the team got lucky. A French source advised Lieutenant Grant Hellman, the team leader, to check out an area near the Giessen River. Hellman rushed to the area and quickly located two of the safes lying in the mud in a large creek.

It appeared that the safes had been thrown into the creek from a stone bridge 100 yards upstream and had washed downstream.

Hellman then began searching the nearby banks for the third safe—it was nowhere to be found.

Buried Treasure

In desperation, Hellman had the creek dammed up; bulldozers were brought in to dredge the bottom—again, no luck. Hellman however, remained devoted in his efforts and decided to conduct one last search.

This time, he noticed something metallic shining in the sun. As he walked toward the object, he realized it was the third safe. Most of it was still buried in the creek bed.

A quick inspection by the Signal Corps determined that there had been no tampering with the materials inside the safe. The search had finally ended and those back at Supreme Headquarters breathed a giant sigh of relief.

Whodunnit?

Shortly after the missing safes were recovered by the unit, Colonel Erskine contacted the French once again to see if they had any clue as to what really happened. He prefaced his questions by stating that he did not want to see anyone punished, he only wanted to get to the bottom of the mystery.

A few days after Erskine's request, the French finally admitted that on the night of February 3, a French military chauffeur, who had lost ***his*** truck, decided to "borrow" the one that the GIs had left unattended outside the "house of ill repute."

The man had gotten scared when he heard about the search and, afraid that he would be accused of spying, he had dumped the safes into the creek. The Allies were eventually satisfied that this was indeed what had occurred.

(Continued on page 12)

(Continued from page 11)

The Human Factor

What is the OPSEC lesson in this amazing tale? Seemingly the Allies had a perfect plan. They knew their adversary, thanks to gargantuan codebreaking efforts; they knew what critical information to protect; and they applied intense security measures to ensure its protection. The one thing they did not consider in their risk assessment was the unpredictability of the human factor.

Consider for a moment, the huge amount of time, effort, and money that went into the SIGABA program. Ponder also the incredible advantage the device afforded the Allies and the huge security apparatus designed and implemented to protect the device.

All of this hard work and planning were almost destroyed—not by a carefully orchestrated commando raid, or a well-designed espionage plan, but by two American GIs who chose to pursue a few moments of pleasure rather than ensure the safety of their cargo and the success of their mission.

As OPSEC professionals we must never forget to factor in the human element. It is a mistake to assume that your OPSEC plan is foolproof, even if it appears that way on paper.

We have to realize that even the best units and organizations are not composed of robots, but of human beings who, despite their best efforts and intentions, can become distracted or led astray at the most critical times.

Make sure you consider this when you develop your OPSEC and other security plans. Never assume that personnel have had too many security briefings. We all need to be periodically reminded of our individual responsibilities. In many cases, the margin for error is zero—constant reminders such as OPSEC posters or other OPSEC products can help drive the message home.

Remember, if you leave out the human factor, you may not be as fortunate as the hapless GIs in this story. You may emerge from your revelry to find that the crown jewels are gone forever. ♦

Cancellation of Chiemsee Regional Symposium

Every year the IOSS sponsors several events, including one or two regional symposia. These smaller events are designed to get to parts of the Federal work force and military members who don't have the time or resources to attend our National OPSEC Conference and Exhibition. We move the symposia to different locations each year in order to make training and professional development opportunities available to our entire customer base. To that end, the IOSS scheduled the Regional Symposium in Europe for December 2000.

Unfortunately, when it came time to sign the hotel contract, five weeks before the symposium, we had only a few registrations. The IOSS determined that it was too great a risk to commit significant dollar and manpower resources for such a very small number of guaranteed attendees; therefore, the event was postponed. There is definitely a customer base in Europe, but we obviously need to go back to the drawing board to come up with a time, place, and marketing scheme to maximize the effectiveness of the symposia.

The IOSS is currently exploring co-sponsorship with theater commands or with other U.S. government organizations. We'd also like information on what training and briefings are needed, or if there are any specific topic areas or themes we should address.

If you are stationed in Europe, or own any resources in theater, please contact us if you have any time, location or agenda suggestions. If you can help "get the word out" once the event is scheduled, please let us know. The IOSS POC is Lynne Clark, who can be reached by email at b.clark@radium.ncsc.mil.

Remembering Former NSA OPSEC Program Director George Jelen

Annual OPSEC for Literature Award Renamed "The George F. Jelen Literature Award"

by Tom Harig
IOSS Staff

The OPSEC community lost an ardent advocate when George F. Jelen, passed away suddenly on September 1 in a Washington, D.C. hospital. He was 64.

Mr. Jelen, a native of Columbus, NE, attended the Industrial College of the Armed Forces. and earned a Master's Degree from the American University.

He served in the U.S. Air Force prior to joining the National Security Agency (NSA) in the 1960's. At NSA, Mr. Jelen spent most of his professional life specializing in cryptography and information systems security.

Career Change

His career took a different turn, however, in 1989 when he returned from a Pentagon assignment to become the manager of the Operations Security organization at NSA, which included the Interagency OPSEC Support Staff (IOSS).

In this assignment, he chaired the National OPSEC Advisory Committee, composed of senior government executives that served as a board of directors providing guidance on the implementation of OPSEC programs throughout the government. He also oversaw its task of establishing a body of OPSEC doctrine that was later published by the IOSS.

Mr. Jelen worked diligently to implement an OPSEC Coordinators organization at NSA and enthusiastically supported the efforts of the IOSS to establish the National OPSEC Conference and Exhibition.

A frequent visitor to the IOSS, Mr. Jelen would often engage the staff in discussions about all aspects of operations security. He sought everyone's opinions, whatever their level of experience, believing that each staff member had a point of view that deserved consideration.

George F. Jelen

A Professional Obligation

Mr. Jelen especially encouraged those with whom he came in contact to publish their viewpoints in their areas of expertise. Mr. Jelen cited several reasons for publishing, noting that writing forces one to think more deeply and critically about a subject.

He believed that it was a professional obligation to contribute to the literature of one's career and that this can inspire new thinking on the part of someone else. In this way, he argued, the profession itself advances.

He wrote a number of articles on OPSEC, including "The Defensive Disciplines of Intelligence," which appeared in 1992 in the *Journal of Intelligence and Counterintelligence.*

Jelen's Legacy

After retiring from government service in 1995, Mr. Jelen remained involved within the OPSEC community, serving as a board member for the OPSEC Professionals Society (OPS).

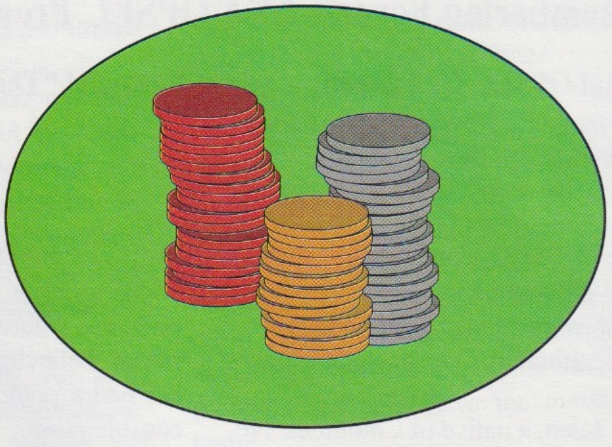
At the time of his death, Mr. Jelen was the head of his own consulting company that worked on systems security issues.

Mr. Jelen left a legacy of strong support for Operations Security. Because of his passionate belief in professional writing, the IOSS has decided to name the National OPSEC Literature Achievement Award after him.

The George F. Jelen Literature Achievement Award will be presented annually at the OPSEC Awards Luncheon held during the National OPSEC Conference and Exhibition.♦

> **"Although there are many ways to contribute to your profession, contributing to the literature of the profession is one of the best."**
>
> **George F. Jelen**

Las Vegas Regional Threat Symposium February 6 & 7, 2001 "A Sure Bet"



Program

The Interagency OPSEC Support Staff and the Department of Energy Nevada Operations Office will host a Regional Threat Symposium at the DOE facility in North Las Vegas on February 6 - 7, 2001.

A one-day seminar, "Counterespionage and OPSEC," will be offered on February 6. This seminar is tailored to OPSEC analysts, and includes a short history on espionage in the United States, adversary HUMINT methodologies, and current issues and events in counterespionage.

On February 7, a series of classified briefings on current intelligence threat topics will be offered, including:

D*I*C*E 2001
Web Content Threats
DoD Web Vulnerabilities: Lessons Learned
Foreign Intelligence Activities
Terrorism & Technology

Accommodations

The following hotels are located near the facility in North Las Vegas.

Texas Hotel & Casino
800-654-8888

Fiesta Hotel & Casino
800-731-7333

If you prefer to stay on The Strip in Las Vegas, the DOE facility is approximately a 20-minute drive.

For a complete listing of Las Vegas hotels visit:
http//www.nowka.com/casinos.html
http://www.lvrs.com

Conference Fee

The fee for the symposium will be $60 for both days, $30 for one day. Fees include lunch and refreshments on both days.

Clearance Requirement

Participants attending briefings on Wednesday, February 7, must hold a current U.S. **SECRET** clearance.

Registration

On-line registration is available at *www.iaevents.com*. Please contact McNeil Technologies at 410-553-6465 to have registration materials mailed or faxed. Read submittal instructions carefully for registration and clearance certification

Contact Information

www.ioss.gov is the IOSS web page, with information on all IOSS events, products, services, and training opportunities.

Visit ***www.iaevents.com*** — the registration site for all IOSS events.

Questions on registration and clearances? Call McNeil Technologies at 410-553-6465.

Questions about the program? Call the IOSS at 301-982-0323.♦

National OPSEC Awards Board Members Selected

by Jim Aycock
IOSS Staff

The Interagency OPSEC Support Staff (IOSS) is pleased to announce the members of the 2001 National OPSEC Awards Board impaneled to judge the coming year's awards contenders. These prestigious awards will be presented at a luncheon during the National OPSEC Conference and Exhibition to be held in Tampa, FL in June.

Board Members

With five new members joining two continuing participants, the panel itself is a winner!

Returning members are Mr. John Kirby of the Immigration and Naturalization Service and A. Reese Madsen of the Coast Guard. The recent additions to the panel are Mr. Pat Geary, President of the OPSEC Professionals Society; Mr. Mike Kane, from the Bureau of Alcohol. Tobacco, and Firearms; Ms. Cathy Kiser, Federal Bureau of Investigations; Ms. Jeannie Ping, U.S. Navy; and Ms. Judy Scherben of the National Security Agency.

Panel members serve a term of two years. Their job is to evaluate innovative applicants from the government and contractor sectors for OPSEC awards in these four categories: Individual, Organization, Multimedia, and Literary Achievement.

The award for literary achievement was renamed "The George F. Jelen Literature Achievement Award," after a former director of the NSA OPSEC Program who passed away in September.

Streamlined Process

Beginning this year, several major changes were made to the award process. Under the new guidelines, *anyone* in an organization can forward an *unlimited* number of submissions, with the approval of the senior official of their organization. Additionally the entire process was streamlined, making it easier and more clear-cut for board members to select the winners.

Criteria

The criteria used by the board to determine the awards include, but are not limited to, the following:

- Evidence of the ability to identify and solve significant OPSEC problems, threats, or vulnerabilities.
- Demonstration of outstanding leadership or creativity in the application of OPSEC.
- The imaginative use of resources (personnel, fiscal or facilities) to accomplish OPSEC goals.
- The application of creativity, innovation, enthusiasm and individual results.♦

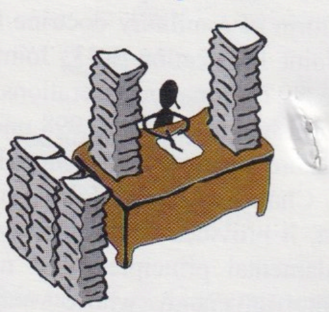
From the Editor

The holidays are over and it is now time to start keeping those resolutions we made with such conviction.

One resolution might be to submit an article for publication. As you read on page 13, an OPSEC pioneer, George Jelen, believed it was everyone's professional duty to publish papers and articles in their areas of expertise to share their knowledge and to inspire others to do the same. The OPSEC Indicator is a perfect venue for unclassified articles on OPSEC or counterintelligence threat issues.

Anyone may submit articles by mail or via E-mail to **ioss@radium.ncsc.mil** or by fax to (301) 982-2913. Submissions to ***The OPSEC Indicator*** are subject to editing for space, clarity and classification.

Lynne Yates



INTERAGENCY OPSEC SUPPORT STAFF

Visit our website at www.ioss.gov

21st Century Adversary's Weapon of Choice Will Be Bytes not Bullets

by Jim Garamone
American Forces Press Service

The United States military is under almost daily attack. The DoD routinely detects 80 to 100 "cyberincidents" on computer systems each day. The department is experiencing sophisticated computer challenges now; one major attack is under investigation.

Changing Technology

DoD officials will not comment further on the attack because it is a law enforcement and intelligence matter. Few people can deny the world is in the midst of an information revolution. Information technology is changing the face of warfare just as the Industrial Revolution did on 19th century battlefields.

DOD Response

The DoD has not been caught napping. Rather, the department has been laying the groundwork for military operations in the cyberworld. It is in the form of a military doctrine known as Joint Publication 3-13, Joint Doctrine for Information Operations.

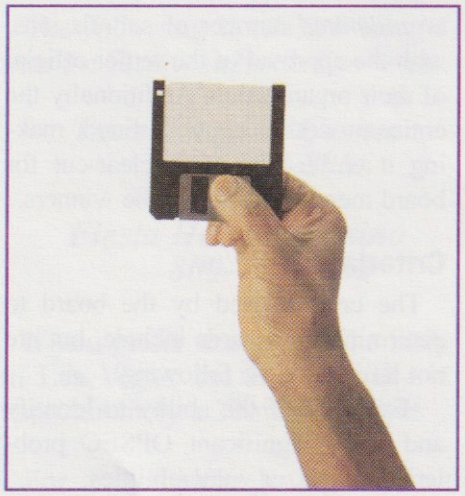
Published in October 1998 under the signature of Army Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, it provides warfighters with the fundamental principles they need to engage an enemy whose weapon of choice is bytes, not bullets.

Information Operations

"Information operations" brings to mind a group of computer hackers hunched over keyboards attacking enemy command and control networks. It is that and much more, said Air Force Brig. Gen. Bruce A. Wright, deputy director of Information Operations on the Joint Staff in the Pentagon.

"Thousands of service members across the military are involved in information operations," he said during a recent Pentagon interview.

Information operations, according to Joint Pub 3-13, "are actions taken to affect adversary information and information systems while defending one's own information and information systems."



Wright said information operations include the use of psychological operations, deception, jamming, and computer network attack and defense. It also includes operations security and electronic warfare.

"Information operations cover the full spectrum of conflict from peace to crisis to war back to peace," he said. "Information operations builds upon traditional military operations, starting with command, control, computer countermeasures.

It's still very easily tied to traditional military operations to degrade the command and control or the information capability of an adversary while fully protecting our own."

Cyberwarfare

Wright said potential enemies' "information abilities" point to a new form of warfare that could threaten the United States."The threat of cyberwarfare is real," he said. "Our potential enemies tend to be multispectral. They're either unpredictable or they're unknown. Clearly, whether terrorist or more traditional, they can be dangerous."

The threat of cyberwar directed against U.S. infrastructure concerns Pentagon planners. "We haven't seen severe impacts on our military capability," Wright said.

"We have seen enough intrusion via telecommunications links or computer network attack, that it certainly makes us watchful. Computer network attack is a real threat." Fueling this is the growth in commercial industry, he said.

"Those elements of industrial power transition into combat capability. You can compare information operations—to the first use of the airplane. The airplane was commercially focused and it eventually moved into a combat weapon," he said.

OPSEC is Key

The first mission is defense. Service members at all levels can help by practicing good operational security, he said. "We've always done OPSEC, whether it was how we protect our phone conversations or now, how we protect our computers."

Wright said,"OPSEC is always a very fundamental element of information operations and protecting our command and control." DoD recently formed Joint Task Force Computer

Network Defense.

The task force, based at the Defense Information Systems Agency here, specifically protects DoD command and control information systems from outside attack — whether it's a teenage hacker or the government of another nation.

The U.S. military is "not out there committed to a capability take-down of another country" through information operations,Wright said. "We will do as we've always done: look for opportunities in a combat environment to degrade the enemy's command and control.

"But more than that, even prior to a combat environment, how do we shape the battle and battlefield? That's important also. It is essential that we are ready to do that and take advantage of opportunities." DoD is integrating information operations into exercises and it is part of contingency plans, Wright said.

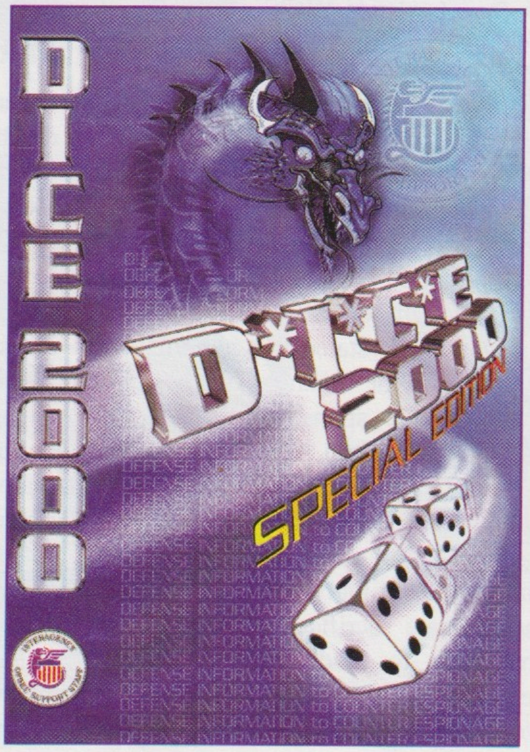
An Evolution

The U.S. military is also working with allies to ensure joint and combined operations consider information operations. He said the release of the joint doctrine is not revolutionary, but evolutionary.

"We've always had these concerns and we always worked these," he said. "What we still have to do is to understand what the information explosion really means. We've got to stay up to speed with what private industry is doing and up to speed on what the adversary is doing and who that adversary might be."♦

The IOSS is accepting orders for the newest IOSS video, "D*I*C*E 2000, Special Edition."

Order by e-mail at ioss.radium.ncsc.mil or send a fax to (301) 982-2913.


DICE 2000
D*I*C*E 2000
SPECIAL EDITION
DEFENSE INFORMATION to COUNTER ESPIONAGE
INTERAGENCY OPSEC SUPPORT STAFF

The OPSEC Indicator

Published Quarterly by

The Interagency OPSEC Support Staff

6411 Ivy lane
Greenbelt, Maryland
20770-1405

Thomas P. Mauriello
Director

Lynne M. Yates
Editor

Telephone
(301) 982-0323
FAX
(301) 982-2913
E-Mail
ioss@radium.ncsc.mil

www.ioss.gov

This is a U.S. Government Publication

Contents are not necessarily the views of, or endorsed by, any government agency.

National Threat Symposium and Security Awareness Fair

Joint IOSS and NACIC Event Boasts Capacity Crowd

by Lynne Yates
IOSS Staff

On November 2, more than 500 individuals from government and industry gathered at the Kossiakoff Center on the campus of the Johns Hopkins Applied Physical Laboratory (APL) for the 12th Annual National Threat Symposium and Security Awareness Fair.

This was the IOSS' 12th symposium but this was the first time that the day-long event was co-sponsored by the National Counterintelligence Center (NACIC). The new partnership made perfect sense from a corporate perspective—the IOSS sponsored its yearly event at APL; the NACIC sponsored a similar event each fall at the same location. Combining forces with NACIC resulted in a comprehensive, cost-effective awareness experience that appealed to a broader base of government and industry professionals.

Security Awareness Materials

After receiving their badges, guests were encouraged to visit the variety of informative exhibits. Before long, guests were returning to their cars loaded down with security awareness giveaways to bring back to their organizations. The consensus was that the exhibits were a treasure trove for security awareness professionals. One attendee commented, "If I learn nothing else today, I've already enhanced my security awareness program for the year by collecting all of these products on display."

Exhibitors included the Defense Security Service; the Defense Threat Reduction Agency; the Department of Energy; the Defense Intelligence Agency; the Federal Bureau of Investigation (FBI); the National Classification Management Agency; the National Reconnaissance Office; the National Security Agency's Security Awareness, Protective Technologies, and Domestic Technology Transfer Offices; the Naval Intelligence Security Advisory Committee; and the Security Awareness and Education Subcommittee. Naturally, the IOSS and the NACIC also had booths on exhibit.

Mr. Steve Argubright, NACIC, and Mr. Tom Mauriello, IOSS, formed a new partnership for the annual symposium.

The group then assembled in the auditorium for the day's briefings. Participants received a heartfelt welcome from Captain Nick Harris, USN, who has oversight of the IOSS at NSA. Captain Harris stated that although he was new to the organization, he fully supported the sponsorship of events like the symposium.

He added poignantly, "I am proud to say that 'purple' runs through my veins ...several of my close friends and associates in the military have had to make the ultimate sacrifice—they lost their lives due to inadequate operations security." Captain Harris' stirring words set the tone for the classified sessions that followed.

The first speaker was Mr. John McGaffin, a retired government official who enlightened the audience on his recent accomplishments as the Chairman of the Special Review Process for counterintelligence known as "CI-21." He was appointed to the job in June 1999 by the Secretary of Defense, the Directors of the Central Intelligence Agency (CIA) and the FBI, and is now implementing the critical recommendations brought to light by the review.

Web Vulnerabilites

Other morning speakers included Mr. Steven Stigall who discussed a multitude of web content threats and Army Major Jim Lyons, of the Joint Web Risk Assessment Cell (JWRAC) who spoke on their efforts to "clean up" the Department of Defense web pages.

A delicious buffet lunch was included in the $35 fee for the symposium. Attendees ate in two shifts which provided further opportunity to network with exhibitors or to view recently produced video presentations.

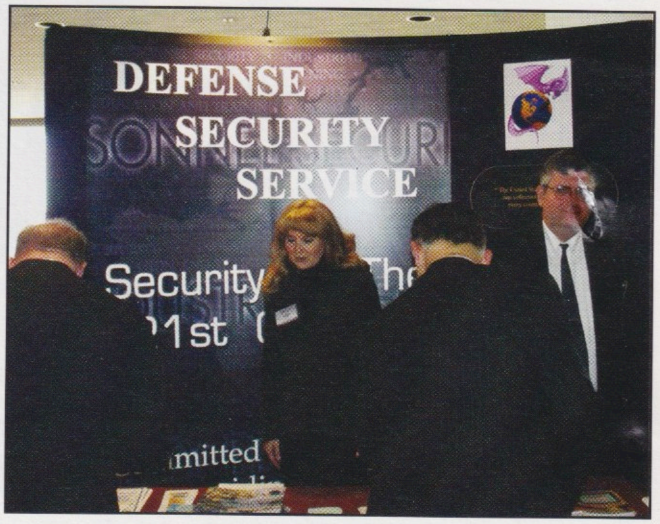
21st Century Threats

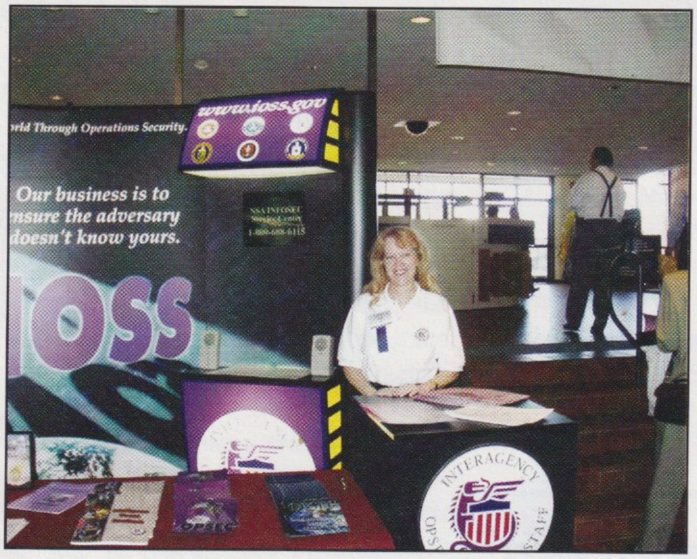
The afternoon concluded with in-depth sessions on the foreign intelligence threat from Army LT COL Jim Stuteville of the Defense Intelligence Agency and on various domestic threats presented by Mr. Michael J. Waguespack, the Deputy Assistant Director, National Security Division of the FBI.

The afternoon's presentations left no doubt that the United States is facing major threats in the 21st century—from domestic terrorists here in the United States as well as from foreign terrorists, foreign governments and foreign intelligence services.

The record attendance, wonderful facilities and tranquil setting convinced planners from the IOSS and NACIC to schedule next year's event at the APL. Look for more details in upcoming editions of *The OPSEC Indicator.*♦

Johns Hopkins Applied Physics Lab was the perfect setting for gathering information, visiting booths, attending briefings and networking.





Quarterly Quote

"Too often we enjoy the comfort of opinion without the discomfort of thought."

—John F. Kennedy
1917-1963
U.S. President

Interagency Opsec Support Staff
6411 Ivy Lane
Greenbelt, MD 20770-1405

First Class Mail
Postage and Fees Paid
National Security Agency
Ft. Meade, MD
Permit No. G-712