PUBLISHED BY THE INTERAGENCY OPSEC SUPPORT STAFF

THE OPSEC INDICATOR

Volume XII

Fall 2002

"Meeting The Challenges of a Changing World"

The Dark Side of Open Source — Data Aggregation Issues

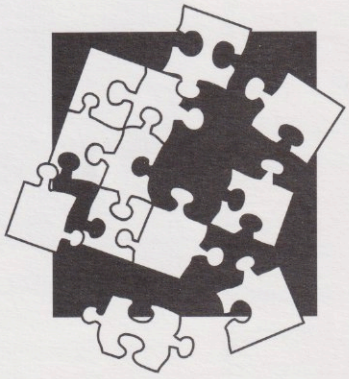
by Lynne Clark
Chief, IOSS Program Development Team

The problem of data aggregation has long been one of the most difficult issues facing those of us who deal with the protection of information. We cannot operate in a world where everything is classified, but we live in a society that has difficulty understanding the value of unclassified information, and how that information can be used against us.

Let's say I work for an organization that operates worldwide, is about 100,000 people strong, and part of our mission is classified. In fact, some of the people in this organization put their lives on the line doing their jobs, and if classified information is compromised, the mission is degraded, and people could die.

Database Vulnerability

My job, however, is to manage communications operations for this huge organization, and one of my main problems is keeping track of pieces and parts, what's operating and what isn't, and how soon things will be fixed. I decide to spend part of my budget on developing a database that will provide me that information in a flash. I distribute the software to all of my subordinates worldwide, and use the Internet as the backbone for accessing and updating the database.



Each individual piece of information that goes into the database is unclassified, so the database is unclassified.

Over time, our little database works so well that others in the organization recognize its utility, and begin to use it to track other types of equipment. We add a chat room feature where maintenance personnel can talk about sharing resources and how to fix various items in our inventory. No single discussion is classified, everyone knows it is for unclassified use only.

Eventually, anyone who can access the database can aggregate enough information to keep tabs on our operations and to predict our plans.

The Unthinkable

Then one day the unthinkable happens. We lose an entire crew (and their equipment) to hostile action. They were fixing a broken communications tower in a remote part of the world. Five are dead, three are injured, and $1.2 million in state-of-the-art equipment is lost or destroyed.

The crew was unarmed because no one thought there was a threat. We discover that there was a previously unknown group of nationalists unhappy with a U.S. presence in their country. They decided to adopt terrorist tactics to advance their cause.

As the investigation progresses, we learn that they've hacked into our database, identified our resources in their country, and used the information in the database to predict when a team would visit their region. All unclassified information but, in retrospect, very vulnerable to aggregation and exploitation by our adversary.

Worth the Investment

Stupid on our part? Not necessarily. Avoidable? Certainly. Costly to fix?

(continued on page 2)

Inside This Issue:

(continued from page 1)

Perhaps, but it may be worth the investment. In fact, it may not be costly in dollars but rather in the time it takes for our people to understand data aggregation issues. It may also be somewhat costly to implement policies and procedures that allow use of the database, but still protect our people and our mission from adversarial action.

This type of fictional situation may not happen every day, but it is not outside the realm of possibility. It is not simply an information management issue – it touches on threat analysis and awareness, physical security, and other issues.

As technology races forward with better, quicker, and cheaper ways of managing information; and organizations embrace the technology before thinking through all the associated vulnerabilities; aggregation issues become increasingly harder to resolve.

Identity Theft

We can find a more personal example in identity theft, which is an important issue today. In this case, an adversary manages to aggregate enough information about you to use your identity to get access to your accounts, create new accounts for which you will be responsible, or commit some criminal act for which you may be charged.

Individuals share enough information to be exploited almost every day. You use a credit card at a store, you pay your bills on-line, you make a reservation over the phone and confirm with a credit card, or worse yet, you make a phone payment with your checking account.

These are all ways that an adversary can collect enough bits and pieces of your personal information to make your life miserable.

This problem has been in the press before and most of us are becoming more cautious about sharing personal information. Although we have been educated about this threat, it is still difficult and inconvenient to function without sharing certain amounts of personal information.

A Classification Issue

Classification experts recognize the potential situation wherein multiple unclassified documents or multiple pieces of unclassified data could become classified when aggregated in a single document, or in a database, or in the possession of a single individual with the expertise to act on the information.

Performing a thorough OPSEC review of information prior to release for OPSEC can protect your mission and save lives.

The provisions of the Freedom of Information Act even address the aggregation principle (to prevent too much information being released to a single requester). The problem is that there are not many good, practical solutions to the aggregation dilemma.

Once aggregated unclassified information borders on revealing classified information, how can appropriate protections be applied?

The Information Age

The Information Age has made the problem worse. It is no longer a matter of tracking which 50 people received a set of documents — in most cases, it is impossible to know how many people had access to specific information. People continue to make the assumption that if information is unclassified it is releasable.

So, what's to be done? Aggregation of unclassified information, with its resulting impact on operations, missions, activities, and personnel safety is a basic operations security (OPSEC) concept. The OPSEC process was designed to identify what information needs protection (critical information); what adversaries are likely to exploit the information (threats); what means an adversary might use to get the information (vulnerabilities); what happens if we lose the information (risk); and what we can do to correct the associated problems (countermeasures).

In other words, OPSEC offers a viable means by which we can protect certain unclassified information before it gets released, before it can be aggregated enough to reveal classified intentions or capabilities.

Timely Controls

Since we can't recover information once it has been released and aggregated, we need to control it before it is released. The usual result from application of the OPSEC process to the release of unclassified information is that much of the original information is still released, but the detail is removed. There are certain categories of information that probably wouldn't hurt us even if they were aggregated.

Most organizations have a need to advertise their existence, to release basic information about their mission, their location, their staff, and about how they do business. However, they probably do not need to release personal details about their staff, or their schedules, plans, specific capabilities, internal methods or regulations, or their lim-

itations.

There is a difference between information released because it is operationally expedient and information released because it is simply convenient.

You might wonder who would publish even unclassified information if it would potentially damage the mission, or threaten individual safety. Well, the answer to that question is that many people are woefully undereducated as to the intelligence value of unclassified information.

No one would intentionally publish or release information known to be harmful to the mission or put the people at risk. However, in the absence of education as to the intentions and capabilities of our adversaries and identification of critical information, how is the average worker to know what to protect?

The Bottom Line

The bottom line is that we will never be 100% successful at preventing aggregation. We can, however, dramatically increase our ability to protect critical information if we accept certain facts about the world in which we live and work.

There are "bad guys" out there who will exploit any information we freely provide. More than 80% of intelligence collected by foreign intelligence services comes from open sources — that is, we give it away.

While we would all like to work in an unclassified, unfettered environment, that world ceased to exist long ago. Most of us only began to accept its demise on September 11, 2001.

The more we develop and use unclassified systems to record, save, and process our information, the more those systems and their information will be exploited by our adversaries.

Technical security systems developed to protect information processing systems are only as good as the next smart guy that finds a way around them. That includes communications systems. The success of encryption, firewalls, and passwords all depend on proper usage. The more we create unclassified databases; the more we publish on the web and the more we think only of what is convenient when conducting business; the more we open ourselves to our adversaries. This allows them to aggregate enough information to gain invaluable insight into our classified or sensitive activities and operations.

Possible Solutions

How do we deal with the issues of aggregation? **We start by acknowledging that unclassified does not equal unimportant.** We need to control certain unclassified information as if it were classified, and remember that if someone with malicious intent aggregates the information, it can cause great harm.

We must develop procedures to implement good, practical OPSEC programs in order to identify what information is critical, who might want it, what we're doing to let them have it, what it costs us, and how we can control the information flow.

We need to educate our people so that they truly understand what information they need to protect and how to do it. We should motivate them by helping them understand the adversary.

And finally, we should remember that when we cannot prevent aggregation, the OPSEC process helps us analyze what's been compromised, and the potential impact to our operations. Once those are identified, we can act accordingly. Ultimately, what we understand, we can deal with. It's the surprises that can really hurt. ■

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
(443) 479-IOSS

FAX
(443) 479-4700

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.

The National Threat Symposium — Beyond Terrorism

December 11-12, 2002

Johns Hopkins Applied Physics Lab
Laurel, MD

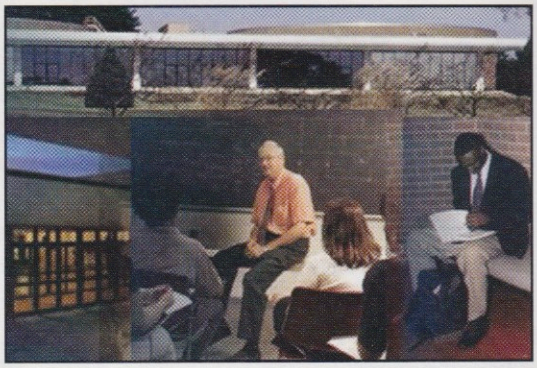
A Two-Day Symposium!

The Interagency OPSEC Support Staff (IOSS), in partnership with the National Counterintelligence Executive (NCIX) will present two days of training, briefings, and networking opportunities with a focus on operations security, terrorist and intelligence threats to U.S. national security, and new techniques for developing security awareness programs.

Wednesday, December 11 - Security Awareness Fair and Training Sessions

The Awareness Fair is an impressive collection of exhibits from government departments and agencies who have resources available to security professionals to assist in the development of security awareness. Many of these exhibits represent organizations with valuable resources available to customers in addition to their awareness products and services.

Training



Several tracks will offer courses, seminars and workshops, including a Terrorism seminar; an OPSEC class on "Risk: The Forgotten Step;" an OPSEC exercise; a DSS security marketing workshop; and the popular "Motivation Through Communication" course, a briefing skills presentation featuring a special appearance by The D*I*C*E Man.

Thursday, December 12 - National Threat Symposium

The purpose of the National Threat Symposium is to provide current information and analysis to practitioners in OPSEC, military operations, security, risk analysis, counterintelligence, and related fields, and to encourage interaction and networking within the community.

Outstanding speakers who are experts on current intelligence threat issues facing national security will be presenting a day of briefings and discussions at the U.S. Secret level.

Clearances

A U.S. Secret level clearance is required to attend the second day of this event. No clearance is necessary to attend the training sessions.

Fees and Registration

The fee is **$80 for both days - $40 per day**. Register online at ***www.iaevents.com***, or call Systematic Solutions, Inc. on 410-691-0032.

Contact Information

Call the IOSS on 443-479-IOSS for additional information. Inquiries sent via e-mail can be addressed to ***ioss@radium.ncsc.mil.*** Find schedule updates at ***www.ioss.gov.***

Director's Message

IOSS To Open New Training Facility

I've got a lot of diverse topics to discuss this time, so here goes!

■ First, I need to ask for your help — the IOSS has hired a consulting firm to perform an objective assessment on all of our products and services. As readers of The OPSEC Indicator, you are probably aware that the IOSS is always looking for better ways to support our diverse customer base. In the coming months, you may asked to fill out a detailed survey. I implore you to fill the survey out completely and honestly and return it to to the consulting firm. The payoff for you is that you will be providing input that will allow us to address your needs and the needs of your organization.

■ The early months of FY03 finds us preparing to open our new IOSS training facility scheduled for completion in December 2002. Once it is up and running, we will teach most of our local courses at this Greenbelt facility rather than at the National Cryptologic School in Linthicum, MD. We have a number of new OPSEC products scheduled to be ready for distribution, and a new "IOSS Associates Program," which is featured on page 8 in this newsletter.

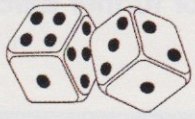
■ As we were closing out the fiscal year (FY) we determined that the IOSS had a 35% increase in customers (from 8,500 in FY01 to 11,500 for FY02). We also taught 82 platform courses to more than 3,800 students; offered 210 OPSEC/Security Awareness presentations to over 40,000 attendees worldwide; and distributed over 125,000 OPSEC products. We saw a new customer set, the public safety sector, emerge after 9/11, and we quickly developed specialized products and training curricula to meet their needs.

■ By now, those of you who have occasion to call us know that the IOSS has a new phone system and new phone numbers. We hope that you find the new system to be customer-friendly and efficient. A major advantage of the new phone system is that we now have Defense Switched Network (DSN) phone numbers. Those of you who have DSN lines can now reach us on *our* DSN phone number, 689-4677.

■ I'd also like to mention how excited and sincerely honored I was to receive the 2002 Presidential Award from the National Classification Management Society (NCMS). It was presented on July 16th at their Annual Training Seminar in Fort Worth, Texas. The IOSS and NCMS have always enjoyed a close relationship and a great deal of cooperation. My sincere thanks goes to NCMS President Dianne Raynor and the members of the Board of Directors for this wonderful and unexpected honor.

■ And finally, The National Threat Symposium and Security Awareness Fair will be held December 11-12, and is co-sponsored by the National Counterintelligence Executive (NCIX). This year's theme is ***Beyond Terrorism*** and we will be addressing the latest adversarial trends and providing valuable threat information. We have also arranged for a variety of training opportunities as well as knowledgeable and lively speakers to educate those involved in the protection of this great Nation. I look forward to seeing all of you there! ■

Tommy



You Can Bet on a Unique Learning Experience!

If You Attend the

West Coast Regional Threat Symposium

February 11-12, 2003 — Department of Energy Nevada Operations Office

Tuesday, February 11

Training

Careful and complete assessment of the threat is critical to the success of any OPSEC analysis. The Threat Research Course will provide 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. Other training will also be available.

Wednesday, February 12

Briefings

The speakers who present briefings at the National Threat Symposium in the fall are invited to speak at the Regional Threat Symposium in February. This maximizes the number of professionals who can benefit from these exceptional presentations.

Fees and Registration

Watch the web for fee information. You can register on-line at www.iaevents.com, or contact Systematic Solutions, Inc. at 410-691-0032.

Clearances

A U.S. Secret clearance is required to attend the event. Please visit www.iaevents.com for further details.

IOSS Training Team Takes OPSEC On the Road

by Charlie Reeder, IOSS Training Team

To satisfy a customer's pressing requirement, Charlie Reeder and Steve Ward, of the IOSS Training and Program Development Teams, respectively, presented The OPSEC Practitioners Course (OPSE-2380) at Stewart Air National Guard Base in Newburgh, New York, in June. Of the 27 students, 25 were from the host unit at Stewart, the 105th Airlift Wing and two were from the 109th Airlift Wing located in Scotia, NY.

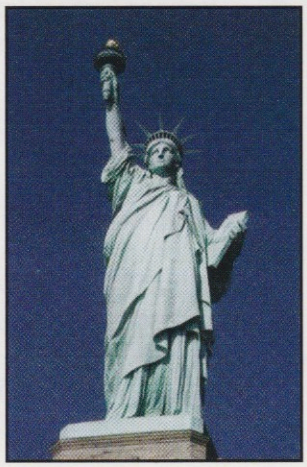
The five-day class was considered a unique and enjoyable learning experience for everyone involved. The level of student participation was high across the board, and the students displayed a serious interest in learning OPSEC techniques. They expressed their intent to return to their units and to begin establishing full-fledged OPSEC programs in order to ensure the Air National Guard is successful in protecting critical information when conducting a mission. ■

On the final day of instruction, the OPSEC Practitioner's class posed in front of a C-5 Galaxy on the flight line at Stewart Air National Guard Base, Newburgh, New York.

From the far left, BG Dana Demand, Commander of the 105th; kneeling in front, Steve Ward and Charlie Reeder of the IOSS; on the far right, Lt Col Carl Adamczak, 105th OPSEC Program Manager; and the rest of the newly trained OPSEC practitioners.

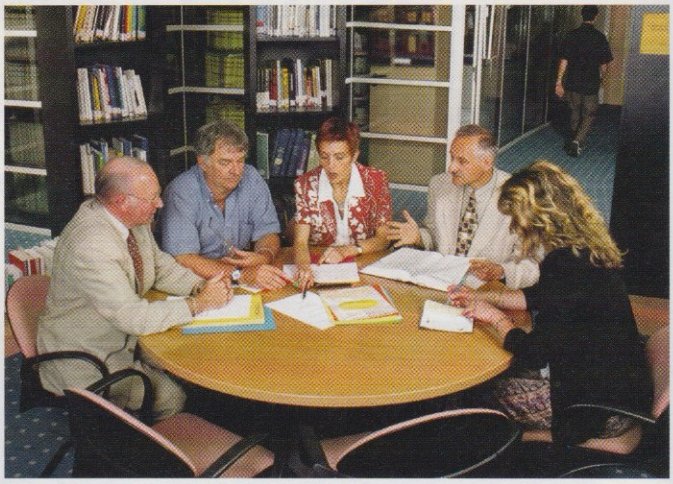
Freedom — no word was ever spoken that has held out greater hope, demanded greater sacrifice, needed more to be nurtured, blessed more the giver, damned more the destroyer, or come closer to being God's will on earth. And I think that's worth fighting for, if necessary.

— U.S. Army General Omar Bradley
(1893 - 1981)



Program Development Team Introduces New Associates Program

by Lynne Clark
Chief, Program Development Team



This fall, the Interagency OPSEC Support Staff (IOSS) has a new initiative designed to help recently assigned OPSEC program managers develop their programs.

The Associates Program will be baselined at four days, and will be limited to six participants in any given week. Candidates will work with IOSS staff and invited experts to tailor their individual programs to achieve their individual goals.

The baseline program will provide a structure within which those individualized program goals will be accomplished. The program is designed to give each candidate sufficient time to work on his own documentation and materials, with the mentorship of an IOSS analyst or instructor.

Candidates will work at their own speed, so the actual time spent at the IOSS facility could be as little as three days or as many as five, depending on the expertise the participants bring to the table and what they hope to achieve.

Candidates will be required to complete either the OPSE-1300 OPSEC Fundamentals Course, the OPSE-1301 OPSEC Fundamentals computer-based training (CBT), or an equivalent course as a prerequisite. The OPSE-1301 CBT will be provided to any applicant who does not already meet this requirement, but must be completed prior to starting the Associates Program.

Candidates will also be required to bring a draft copy of their OPSEC documentation including: an appointment letter, an outline of OPSEC policy, a critical information list, and a statement of management's objectives for the OPSEC program. Detailed instructions on preparation of these drafts will be provided when a candidate is accepted into the program.

All candidates who successfully complete the program will leave the program with the following documentation:

- Draft OPSEC Program Plan
- Draft Threat Assessment
- Refined Critical Information List
- Tailored Awareness Training Package (designed for the general population)

Depending on programmatic need and individual expertise levels, associates may also produce the following documentation:

- Draft Assessment Plan (as appropriate)
- Draft OPSEC Plan (as appropriate)
- OPSEC Training Materials (designed to train working group or coordinators)
- Tailored Briefing Slides (designed to a specific organization or group)

Candidates who successfully complete the program will receive a certificate from the IOSS.

The Associates Program is a practical, hands-on mentorship program and does not address in-depth the material presented in the courses certified by the National Cryptologic School. While one of the basic courses is a prerequisite to the Associates Program, the program is not intended to take the place of the IOSS OPSEC curriculum. Graduates will still benefit from any of the advanced instruction. The baseline 4-day program is outlined below. Adjustments will be made to tailor the program to the needs of participants.

	Group	Individual
Monday		
Introductions, overview of the Associates Program schedule	x	
Review OPSEC basics	x	x
Tailor individual schedules		x
Finish homework (as required)		x
Threat research instruction	x	
Students conduct threat and/or open source research		x
Tuesday		
OPSEC Program Plan contents and format review	x	
Begin work on individual draft Program Plans		x
Wednesday		
Guest speaker/field trips	x	
Awareness training instruction	x	x
Identify awareness training materials requirements	x	
Develop awareness training materials	x	
Develop training materials (as required)	x	
Thursday		
Develop an OPSEC Plan or OPSEC Assessment Plan (as required)		
Analysis skills development tutoring		x
Wrap up/Graduation	x	

Scheduled dates for the Associates Program are:

November 18-21, 2002

January 27-30, 2003

March 3-6, 2003

June 16-19, 2003

August 11-14, 2003.

Application instructions are provided on the IOSS web site at ***www.ioss.gov.*** Additional dates will be scheduled as needed. Candidates may also call the IOSS at 443-479-4677 for further information.

It Don't Mean A Thing If It Ain't Got That Swing!

by Patrick D. Weadon, NSA Historian

When co-workers or friends hear that I write articles about OPSEC, their first response inevitably is, "OPSEC! What the heck is *that*?"

Often I take the direct approach and enlighten them regarding the 5-step analytic process, but on other occasions I relate a theory I have entertained for many years about the proper way to develop an effective operations security plan — that OPSEC is a bit like big band music.

OPUS 1

In the mid 1930's, American musical culture saw the rise of 12 to 18 piece orchestras made up of various combinations of saxophones, trumpets, trombones, clarinets, a stand-up bass, sometimes a guitar and, most importantly, a hot drummer.

Many of these bands played a white bread version of jazz — it was safe and designed not to offend the sensibilities of the general public. If you are old enough to remember Guy Lombardo's sweet version of "Old Lang Syne" you have a good idea of what this kind of music sounded like.

Big Band Brass

In time, many of these mostly white musicians began tweaking their arrangements with the goal of emulating the sound of black bands led by popular favorites like Fletcher Henderson or Chick Webb. Both of these men and other jazz artists of the day were strongly influenced by the incomparable Louis Armstrong.

The Dipper

Armstrong, an orphan from the streets of New Orleans, revolutionized the world of popular music by presenting a kind of music not heard before. His style was a combination of African rhythms mixed with the varied sounds and cadences of the American South. But the key to his music was that his magnificent trumpet playing combined with a rough but seemingly effortless vocal style featured a unique technique known as ***improvisation***.

Louis Armstrong was obviously not the first to improvise on a musical instrument, but he did it so well that he helped elevate it to a popular art form. Armstrong's magic was based on his ability to stay within the confines of the musical work, while at the same time "swinging" or improvising as he went along.

Armstrong could take a trite and mundane melody like "Mary had a Little Lamb" and through improvisation completely transform it.

His playing took simple musical notes and wove them into into something special. He had a knack for playing above and below the melody line moving musically up and down, back and forth, until a simple children's nursery rhyme turned into a jazz masterpiece.

Armstrong could play "Mary Had a Little Lamb" a hundred times and with his incredible talent for improvisation, it would sound different each time. But despite his genius, Armstrong was, like many black musicians of that time, held back by the evil specter of segregation. Countless musicians of all colors recognized his greatness, but Jim Crow kept him from gaining the widespread exposure he deserved until many years later. At that time, however, men like Benny Goodman, Artie Shaw, and other talented white musicians started to take up the banner and began incorporating "The Dipper's" magic into their own work.

As a result, the music known today as jazz became transformed from a largely African-American entity to an art form that was accepted and appreciated by mainstream America and eventually the entire world.

Swing, Swing, Swing

Goodman and Shaw's recognition of improvisation as the key to exceptional music made their bands national sensations. There was no longer any need for them to always play it straight and sweet (a la Guy Lombardo).

Great soloists, like Goodman's lead trumpet player Harry James, developed their talent to the point that they inspired the whole band to *swing* (meaning that the entire band is playing together with incredible drive and passion).

When a big band was really swinging, musicians would often be off on their own musical adventures, but the orchestra as a whole presented a tight harmonic musical wall of sound that made it difficult for even the most reticent soul to sit still.

Like a military unit in the field, when they were on the road, the big band musicians ate, slept and basically spent just about every waking moment together.

Recording was an important part of their business, but to really reach their audiences they were required to travel across the country on cramped busses, sometimes playing 5 to 10 shows a day in the biggest cities and small towns.

If you were lucky enough to get a ticket to see The Benny Goodman Orchestra in Clear Lake, Iowa; you could be sure that the songs that the King of Swing would play that night would sound slightly different from what you heard on the radio.

This was because, on the road, the soloists were free to cut loose. On these occasions, great musicians like Harry James would play their instruments with such intensity that they would whip the huge crowds into a frenzy.

A Different Kind of Perfection

Benny Goodman insisted on perfection from every member of the band. This insistence on perfection was a bit oxymoronic because as Goodman knew better than most, playing swing music is not like playing Beethoven's 9th Symphony — there is never really a right or wrong way to play.

Even so, during rehearsals and recording sessions, Goodman would constantly remind his musicians that "You guys don't need the notes, so don't *read* the notes, PLAY THEM!"

In the words of Goodman's biographer, Ross Firestone, *"The idea was to achieve a style of performance that was tight but also loose, controlled but also free, precise and predictable, yet also open to individual expression."*

Coda for OPSEC Professionals

What can the OPSEC professional learn from Goodman's admonition to his band? Plenty! How many times have we simply gone through the motions in putting together our OPSEC plans just to meet a requirement of our management or chain of command?

The Incomparable Louis Armstrong

How many times have we applied the 5-step process, not with passion and imagination, but in such as way as to avoid "screwing up."

Of course, like great jazz music, great OPSEC requires improvisation, as well as imagination. Like jazz musicians, our work requires that we operate within a certain structure.

We are not often free to shut down our facilities or throw a huge blanket over an aircraft carrier just because an adversary might be watching our every move.

We cannot move the Statue of Liberty or the Washington Monument to Iowa — there are definite limits as to how far we can go. But, as aptly demonstrated by Louis Armstrong and other pioneers of jazz, ***there are no limits to improvisation!***

When you put together an OPSEC plan, don't be afraid to depart from the "melody." Remember that the reason fans adored Harry James was that they never knew where he was taking them musically. Every note was a surprise. This brought a freshness and a vitality that was crucial to the success of his music. In the same way, we must strive to bring the same originality and creativity to *our* work.

If we do, our adversaries will have a difficult time attempting to guess where we are going and what we are trying to accomplish.

Good OPSEC Is Unpredictable

Being predictable can have devastating consequences. The terrorists who attacked our Nation a year ago were depending heavily on our propensity to "play it straight."

Like an aficionado of classical music that is always played the same way, they anticipated our every note and nuance (in addition to our timing).

In the end, they were able to use this to strike against us. If we are to prevail in this long-term struggle, we need to be less like Beethoven and more like Louis Armstrong.

A great jazz solo is unpredictable, but also makes for great music. In the same fashion, a great OPSEC plan should appear unpredictable to the observer but make complete sense to the individual calling the shots.

Remember, for one solid year prior to the attack on Pearl Harbor, the ships of the U. S. Navy's Pacific Fleet left port on Monday morning and returned on Friday or Saturday. Talk about playing it straight! With this schedule, it was no problem at all for the Japanese to determine that the ships would be at anchor on Sunday morning.

(continued on page 12)

(continued from page 11)

Think what a little improvisation would have done. We know now that had the U.S. Navy changed its schedule even a few times that the Japanese high command might have called off the attack in fear that the Kido (attack-force) would get to Pearl Harbor to discover that nobody was home.

Our inability to be imaginative and to periodically change our routine led to our defeat that day.

In our current war, it is imperative that we be innovative, imaginative and above all, *proactive* rather than reactive.

We must strive to not just "read the notes" as Benny Goodman said, but to play them as we have never played them before.

Don't Play It Safe

We might also want to incorporate the philosophy of the late Artie Shaw, another great bandleaders of the Swing era. Shaw was not only an outstanding musician, but a bit of an intellectual as well.

Near the end of his life, he was asked his opinion of the Glenn Miller band. Shaw replied that he didn't have a great deal of respect for the Miller band because in his words, "When they played a song, they never ever made a mistake ... they played it safe all the time ... they never tried to extend their musical talent or horizons."

It was evident to Shaw that the Glenn Miller band was more interested in being popular than in being the best they could be.

Shaw's band rejected this philosophy. Many times when they were on the road, they would experiment with new and challenging material. The fans would often boo them when they declined to play their big hits, but Shaw dismissed them as morons.

He never wanted to be merely satisfied. He always believed that, no matter how good his band was, it could always improve – but only if they tried new and different approaches to the music.

As we enter the second year of our struggle to preserve freedom, follow the example of the great innovators of jazz — push the envelope, take risks, and above all when you lay out your OPSEC plans don't forget to *improvise.* That's what your adversaries are going to do. ■

Record Year for IOSS Training Team

by Gary Manning, Chief, IOSS Training Team

What a busy year for the training team! With new customers and the war on terrorism, the demand for OPSEC training went through the roof.

The IOSS provided 86 training sessions this past fiscal year (FY) 2002 for almost 3,000 students. The training sessions were conducted at the National Cryptologic School (NCS) and at over 30 locations worldwide, supported by the IOSS' mobile training team.

The IOSS also completed major revisions and updates of the Web Vulnerability Seminar (OPSE-2350) and OPSEC Program Manager's Course (OPSE-2390) during FY 2002. A brand-new course, Threat Research for OPSEC (OPSE-2330), will continue as the pilot course during FY 2003.

The OPSEC Practitioner's Course, OPSE-2380, was also recently revised. The first day of OPSEC Fundamentals has been incorporated into the advanced portions of the course, thereby eliminating most of the fundamentals repetition in the course.

Expanded blocks of instruction on Program Development, OPSEC Planning and Surveys have also been included in the revision.

These revisions are based on student and instructor comments from course critiques. The revised course will be implemented at the start of FY 03.

Our NCS training schedule for FY year 2003 can be found on ***www.ioss.gov*** and printed schedules are also available upon request.

Remember, all courses of instruction offered by the IOSS at NCS are available to be supported by a mobile training team at the customer's location of choice.

In addition, to better serve our customers, the IOSS has leased additional space adjacent to our facility in Greenbelt, MD to house a new training center. Our courses will be held in the new training facility beginning in 2003. Students will be advised of their course location by the National Cryptologic School registrar.

For additional information, please call the IOSS Training Team at (443) 479-4677 (Press 1). ■

Upcoming Training Courses and Symposia

2-6 December	OPSE2380, OSPEC Practitioners Course	Linthicum, MD (NCS)*
11-12 December	**National Threat Symposium**	**Laurel, MD (APL)**

2003

6-10 January	OPSE-2380, OPSEC Practitioners Course	IOSS, Greenbelt**
13-16 January	OPSE-2390, OPSEC Program Managers Course	IOSS, Greenbelt
3 February	OPSE-1300, OPSEC Fundamentals	IOSS, Greenbelt
4-6 February	OPSE-2330, Threat Research for OPSEC	IOSS, Greenbelt
11-12 February	**Regional Threat Symposium**	**Las Vegas, NV (DOE)**
19-20 February	OPSE-2350, Web Content Vulnerability	IOSS, Greenbelt
24-28 February	OPSE-2380, OPSEC Practitioners Course	IOSS, Greenbelt
7-11 April	OPSE-2380, OPSEC Practitioners Course	IOSS, Greenbelt
14-17 April	OPSE-2390, OPSEC Program Managers Course	IOSS, Greenbelt
21-23 April	OPSE-2330, Threat Research for OPSEC	IOSS, Greenbelt
24-25 April	OPSE-2350, Web Content Vulnerability	IOSS, Greenbelt
1 May	OPSE-1300, OPSEC Fundamentals	IOSS, Greenbelt
19-23 May	**National OPSEC Conference & Exhibition**	**San Diego, CA**

* **NCS**: National Cryptologic School, Elkridge Landing Road, Linthicum, MD (near the Baltimore/Washington International airport)

****IOSS, Greenbelt:** The new IOSS training facility is scheduled for completion in December 2002. If it is not completed, classes will be held at the NCS.

Note 1: All IOSS classes require a SECRET clearance. Classes can be taught at the unclassified level with prior coordination.

Note 2: All courses listed can be tailored to your group and presented at a location of your choice. Contact the IOSS Training Team at 443 479-4677 (Press 1) to arrange for tailored classes.

Note 3: Directions and clearance procedures will be provided with the registration confirmation.

Class size is limited — register early!

Visit our web site at ***www.ioss.gov*** *for the training form or additional registration information.* ■

IOSS New Phone Menu Options

To better serve you, the IOSS has installed a new, more efficient phone system - now you can directly contact the IOSS team you need, the IOSS executive staff, the office manager or, if you are a new customer, or need to discuss your requirements, you can contact the IOSS Services Coordinator.

Just dial 443-479-4677 and let the menu direct you! The new FAX number is 443-479-4700.

Here are the new menu choices:

Press 1 - Training Team - for information regarding IOSS training courses or the National OPSEC Awards Program.

Press 2 - Marketing Team - for information regarding The OPSEC Indicator, the development of IOSS videos, publications or IOSS events like the regional symposia or The National OPSEC Conference and Exhibition.

Press 3 - Program Development Team - for information on the Associates Program. OPSEC assessments, surveys or help in developing an OPSEC program for your organization.

Press 4 - Product Distribution - for IOSS product requests (videos, publications, training calendar, etc.) or to check on the status of your order.

Press 5 - Executive Staff - if you would like to speak with the IOSS Director, Deputy Director, or Executive Officer.

Press 6 - Office Manager - for general IOSS questions and to schedule the D*I*C*E man's briefings.

Press 7 - Services Coordinator - If you are a new customer or would like to discuss the best way to resolve your OPSEC needs, you will want to speak to the IOSS Services Coordinator who will assist you. ■

From The Editor

In the last issue, I mistakenly referred to the U.S. Marines in my column on incorporating OPSEC in mission planning. Naturally, my alert readers set me straight and reminded me that it was the U.S. Army that fought so valiantly in that conflict in Somalia.

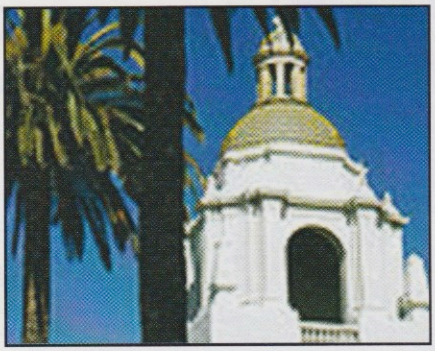
As one of my all-time favorite columnists, the recently departed Ann Landers, used to say, "Thirty lashes with a wet noodle for me!" Thanks for keeping me on the straight and narrow!

– Lynne Yates

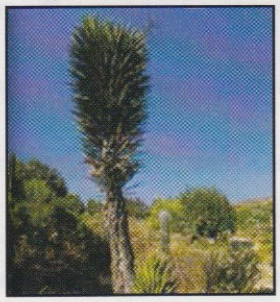
Mark Your Calendar

2003

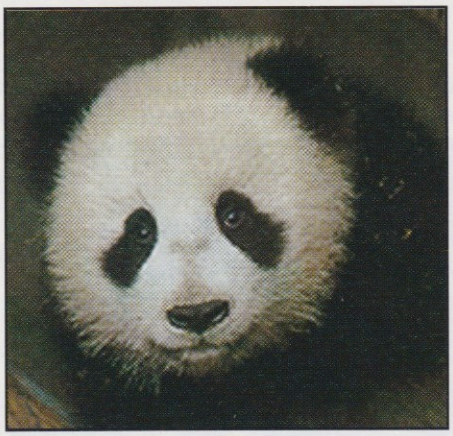
National OPSEC Conference and Exhibition



May 19 - 23, 2003
Town and Country Resort
San Diego, CA



NATIONAL OPSEC CONFERENCE AND EXHIBITION



Join us in San Diego for a week of outstanding briefings, workshops and exhibits.

Register online at
www.iaevents.com

For more information contact:
Systems Solutions, Inc.
Phone: 410-691-0032

George Stephan's

10 Commandments for the OPSEC Professional

I. Thou shalt take the adversary's viewpoint.

II. Thou shalt state critical information precisely.

III. Thou shalt protect your critical information.

IV. Thou shalt know that the 5 steps of OPSEC are not sequential.

V. Thou shalt avoid tunnel vision – see the big picture.

VI. Thou shalt focus on predictability and observables.

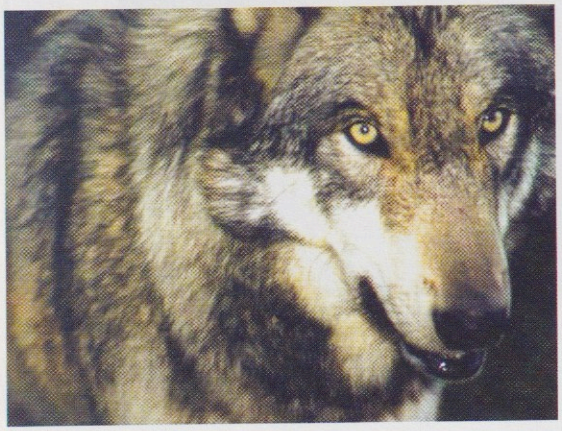
VII. Thou shalt beware — OPSEC and intelligence are often competitors.

VIII. Thou shalt never assume traditional security measures will be sufficient.

IX. Thou shalt use experts for denial and deception countermeasures.

X. Thou shalt remember that OPSEC isn't just security— it's operational effectiveness.

— by George Stephan, IOSS



Coming Soon!!!

"Think Like The Wolf"

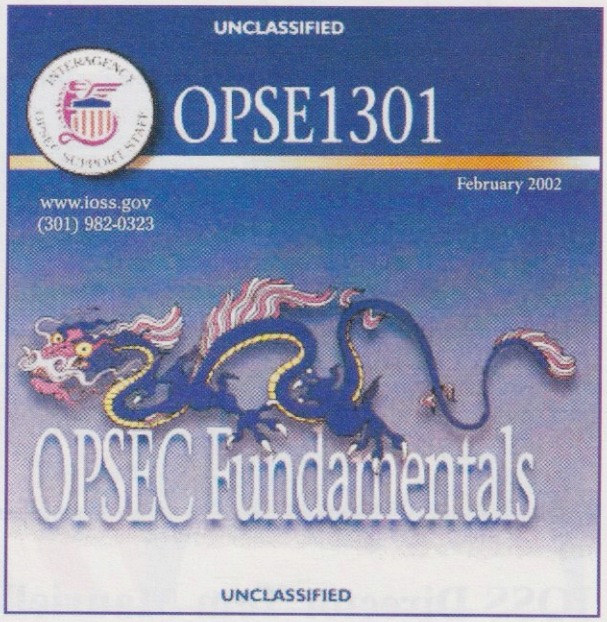
IOSS to Release New OPSEC Video tailored for U.S. Military Operations.

Watch the website for availability!

IMPORTANT UPDATE FOR OPSE-1301 CBT USERS!

Technical Notes for Customers Using Internet Explorer 5.5

by Erin Anderson, IOSS



It has come our IOSS' attention that a small portion of our customers are having trouble using our new computer-based training, OPSE-1301.

We investigated and learned that Internet Explorer 5.5 and later versions introduced a new "feature" which does not allow the user to maximize/minimize a pop-up window when restricting resizing.

This new feature has bitten OPSE-1301 only when run using a display resolution size of 800x600 and only with Internet Explorer (Netscape Navigator does not have this feature).

The glitch appears when the customer can't see/use the navigation aids at the bottom of the course pop-up windows.

Fortunately, this is easily resolved using the following instructions. Choose only one option — whichever one best suits your needs.

Option 1

Change the monitor screen work space from 800x600 to 1024x68. This will make the windows and icons smaller but still viewable within reason.

Right click on your desktop workspace (blank screen area of your monitor with no windows open).

Left click on Properties.

Left click on Settings.

Look for the section of this window titled Desktop Area. If it says 800x600, left click and drag the slider bar to the right until 1024 x 768 pixels is visible.

Left click on Apply. If you get a message saying you didn't test, ignore by left clicking on OK.

Left click on OK of the Display Settings Pop-up window.

The monitor screen will blink for a second or so and then will make the change to the new resolution of 1024 x 768.

Left click on OK.

Option 2

Auto hide the bottom task bar (with the Start button) by auto-hiding the bar goes away when you need it to go away so you can view the navigation aids, but it comes back when you move your mouse over it so you can still use the features on the bar.

Right click in an open space on the bar going across the bottom of your monitor screen (task bar) — do not right click on an icon.

Left click on Properties.

Left click on Auto-hide so that there is a checkmark in the box.

Left click on Always on Top so that there is a checkmark in the box.

Left click on OK.

Once again, these instructions are only applicable for those using Internet Explorer 5.5 or greater *and* a display resolution size of 800 x 600. We hope you enjoy your OPSEC CBT and find it useful in your work. ■

Occasionally, CBT customers also experience difficulty printing out the certificate of completion. As yet, we have not been able to duplicate this situation. If you encounter a problem with the certificate please feel free to contact the IOSS at (443) 479-4677 (*press 2*).

Dragontalk

The IOSS has been receiving unprecedented cooperation from agencies throughout the government. As a truly interagency organization, we will soon be welcoming new assignees from the Federal Bureau of Investigation and the General Services Administration.

These individuals, like our other detailees, will be trained in all aspects of the OPSEC process and in heading an OPSEC program with the idea that they will return to their parent organizations and become that agency's focal point for operations security.

Look for their bios in the next edition!

Linda Heaton, an IOSS team member and contractor for ACS, Inc., has been working part-time for the training team since last June.

She has accepted a full-time position on the marketing team as the IOSS' new conference coordinator (although still a contractor for ACS). Her outstanding organizational skills will be an asset in her new assignment. Congratulations, Linda!

Carla's Corner

To keep that "critical information" flowing smoothly from us to you, please make sure to keep your contact information up-to-date.

Also, If you're moving on and happen to know who your replacement will be, let us know.

You can provide the current data by e-mailing the IOSS at ioss@radium.ncsc.mil.

For any information on IOSS products, please feel free to call me, Carla Colson, the IOSS Product Distribution manager, on (443) 479-4677 (press 2).

IOSS Director Tom Mauriello is Recipient of 2002 Presidential Award

Tom Mauriello and NCMS President Dianne Raynor at the awards presentation in Texas.

The National Classification Management Society (NCMS) presented its 2002 Presidential Award to IOSS Director Tom Mauriello at its annual seminar in Fort Worth, Texas, in July.

The award recognizes extraordinary or unique contributions made to the society or to the Information Security profession by an individual or an organization.

The citation commended Tom's outstanding counterintelligence and security education support to industry and the security community. It also recognizes his valuable contributions and exceptional support to the many NCMS seminars and members throughout the country.

Dianne Raynor, NCMS President, addressed the audience prior to presenting the award to Tom. Raynor stated, "Tom is an unselfish leader and nationally recognized educator. Many have benefitted from his work, marveling at his knowledge and ability to break down barriers and perceptions of security. He has shattered stereotypical methods and approaches to security education."

Among the previous award winners was the IOSS' own Ray Semko (The D*I*C*E Man). ■

The National OPSEC Awards Program
Call for Nominations

The Interagency OPSEC Support Staff (IOSS) is now requesting nominations for the 2003 National Operations Security Awards.

These awards are designed to recognize those individuals and organizations that have excelled in the practice of OPSEC during the past fiscal year.

Through this awards program, the IOSS hopes to encourage the development of new and exciting OPSEC programs and awareness products. The continued success of this awards program rests upon your support as we seek to recognize excellence in OPSEC.

The National OPSEC Awards Program nomination booklet may be found on our web site at **www.ioss.gov**. The five award categories are: Organizational Achievement; Individual Achievement; Multimedia Achievement (Electronic); Multimedia Achievement (Print); and Literature Achievement.

All award winners will receive official recognition at a formal awards dinner during the 14th National Operations Security Conference and Exhibition to be held on May 19-23, 2003 in San Diego, California.

Nominations, including those for contractor organizations and individuals, may be made by any component within those government departments and agencies assigned, or supporting, a national security mission. The IOSS requests receipt of nominations by the close of business on December 31, 2002.

Should you require any further information concerning the National Operations Security Awards Program, to include eligibility and nomination procedures, please call Mr. Charlie Reeder, the Awards Program Administrator, on (443) 479-4726 or DSN 689-4726. ■

Visit our website at www.ioss.gov

Quarterly Quote

"A great many people believe they are thinking when they are merely rearranging their prejudices."

— William James
American Author and Philosopher
(1842-1909)

Interagency OPSEC Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405

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