Protection of Critical Information Key to Success in Battle of the Bismark Sea

by Patrick D. Weadon
NSA Historian

The morning of March 3rd, 1943 dawned clear and bright on the Japanese convoy making its way through the Bismark Sea to the island of New Guinea. Sent from the massive naval complex at Rabaul, the group was composed of eight troop transports escorted by eight destroyers.

Its mission was to quickly transport more than 4,000 Japanese soldiers to the area around the town of Lae, on the northern New Guinea coast.

The officers and men aboard the ships hoped to be able to breathe new life into a planned Japanese offensive against renewed Allied attempts to control the region. Every man aboard realized that the battle for the island was at a crucial point, and that Japan desperately needed to regain the initiative or risk losing the battle for New Guinea.

The Beginning of the End

Almost from the moment General Douglas MacArthur arrived in Australia in February 1942 (after fleeing the Phillipines on the orders of President Roosevelt), he realized that the massive island of New Guinea would be the key to jumpstarting a massive counterattack against Japan in the Pacific Theater.

If the Allies could prevent Japanese forces from using the island as a staging area to attack Australia, it would be difficult if not impossible for Tojo and his compatriots to deal any kind of finishing blow to MacArthur's efforts.

If, on the other hand, Japan could wrest control of the island, and more importantly the sea lanes in and around the region, Australia and the Allied forces in the area would be in grave danger. Not only would Japan be able to attack major population centers in Australia, they would also be able to shore up the Empire's southern flank in such a manner that a herculean effort would be required to prevent the region from falling within the boundaries of the "Japanese Empire's Greater East Asia Co-Prosperity Sphere."

The effort to reinforce the surrounding area was a last desperate effort to try to win back the island of New Guinea for Japan.

In January 1942, the crucial town of Buna had fallen to the Allies. Now it appeared that General MacArthur's forces would have an opportunity to drive the remaining enemy forces into the sea.

The Green War

This was not good news for the Australian and American troops on New Guinea who had fought so hard to bring the battle at Buna to a decisive end. The island of New Guinea was in short, a hellish place. Brigadier General Pat Casey, an advisor to MacArthur at the time, noted that "he didn't see how human beings could live there, much less fight there."

William Manchester, in his book, *American Caesar* describes the conditions faced by the men who fought in what Manchester describes as "The Green War."

Manchester states:

"It wasn't until they (the soldiers) landed and ventured into the rain forests on steep, slippery root-tangled trails that the full horror of life there...struck them. Blades of grass seven feet high could lay a man's hand open as quickly as a scalpel. The jungle was studded with mangrove swamps, thick clumps of bamboo, and palms. Often, the trail was covered with waist-deep slop. The air reeked with vile odors — the stench of rotting undergrowth of stink lilies...when the rain stopped and the sun appeared, vast suffering waves of steam rose from the dank marshes...bugs were everywhere ... pythons and crocodiles lurked in the bogs...for every man suffering from a gunshot wound, five were laid low with illness...no one was hospitalized unless his fever rose above 102."

In short, the longer the fight for New Guinea took, the longer these brave men had to endure these horrible conditions.

Bushwhacked

Thankfully, the massive convoy that carried Japan's last hopes for winning the island for their Emperor would never reach Lae. Unknown to the Japanese command, the combined efforts of Allied codebreaking units had intercepted critical information on the convoy's intentions and had informed MacArthur's command of their coming.

Seizing the opportunity, MacArthur ordered General George Kenney, his air operations chief, to attack the force as soon as possible. Kenney, whose air exploits would make him a legend in the Army Air Corps by war's end, went to work in his usual style.

Due to the outstanding intelligence provided, the convoy was not hard to find. On the morning of the 13th, waves of American B-17 bombers

PUBLISHED BY THE INTERAGENCY OPSEC SUPPORT STAFF

THE OPSEC INDICATOR

Volume XI

Spring 2001

"Meeting The Challenges of a Changing World"

IOSS and DOE Nevada Host 2001 Regional Threat Symposium in Las Vegas

by Lynne M. Yates, IOSS Staff

The Interagency OPSEC Support Staff (IOSS) and the Department of Energy (DOE), Nevada sponsored a Regional Threat Symposium for Operations Security (OPSEC) professionals on February 6 and 7 at the DOE facility in Las Vegas, Nevada.

Approximately 140 individuals from government and private industry interested in the latest threat information attended the dynamic and informative event.

After receiving their badges on the first day, attendees visited the IOSS booth to pick up OPSEC posters, computer based training CD's, notepads, videos and *The Intelligence Threat Handbook.* Orders were taken for any other products requested that were not on hand. Many participants were enthusiastic that the "D*I*C*E 2000" video was now available.

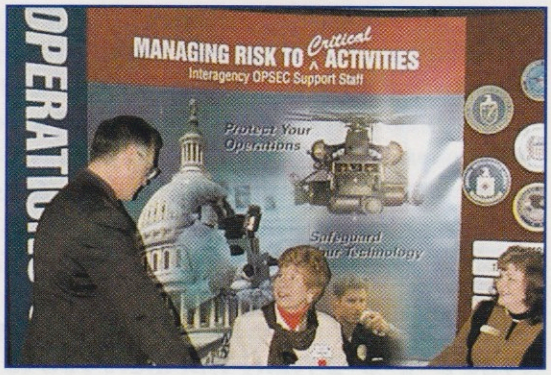
After a continental breakfast, the participants settled in for a day-long training session on "The Peoples' Republic of China Intelligence Strategies From An OPSEC Perspective" presented by Dr. Paul Moore and Mr. John Gaskill of the Centre for Counterintelligence and Security Studies.

Dr. Moore gave an in-depth presentation based on his 20 years of experience in the field as an analyst for the Federal Bureau of Investigation. He began his presentation with a discussion of the Wen Ho Lee investigation. Wen Ho Lee was, coincidentally, a DOE employee accused of espionage who eventually pled guilty to one felony count of downgrading nuclear weapons design secrets to a non-secure computer at the Los Alamos National Laboratory on September 13, 2000.

The Wen Ho Lee Case

Dr. Moore stated, "The main problem in this case was that the government was trying to fit the products of its counterintelligence investigations into a prosecutable package."

"The counterintelligence investigative process is driven by suspicion, but prosecution is driven by proof. As the investigators looked into Lee's activities they found more and more reasons to be suspicious of him, but not actual proof of espionage. They had far too much information to halt their investigation but far too little to carry it forward into an espionage prosecution.



The IOSS Staff gets ready to furnish information and the latest IOSS products at their booth at the Regional Threat Symposium.

"My thesis regarding PRC espionage in general is that China's way of doing intelligence work normally does not leave in its wake the sort of evidence (money, documents, secret meetings with intelligence officers) that juries find most convincing in espionage cases.

"Investigators thus find themselves with a task similar to trying to move an immovable object when it comes to investigating PRC activity with a view to espionage prosecution."

(continued on page 6)

Inside This Issue:

IOSS Presents New Security, Counterintelligence, and OPSEC Awareness Video

This UNCLASSIFIED video is a security awareness tool that offers an assortment of hot topics of interest. From computer security and other challenges brought on by the recent explosion in information technology, to tips for safe travel in a dangerous world, this video offers something for everyone involved in protecting our Nation's security.

The 2-hour video is designed to be viewed in whole or in part as time permits. Each of the following segments is self-contained and offers insights into, and solutions for current issues facing the U.S. government, military, law enforcement, and private industry.

Burning Issues

If you are not diligent about computer security, you are playing with fire! If you're in a hurry, you may become careless with classified material. Poor judgement or unsafe practices could well mean your dismissal. For you, it's career disaster—for the government, it's a loss of technological advantage. This segment exposes how compromising security for convenience damages careers as well as national interests. Produced by the National Reconnaissance Office (NRO).

Expect The Unexpected

At some time in your career, you may travel abroad for business—or you may choose to visit a foreign country for recreation. Do you know how to protect yourself from becoming a target of a foreign intelligence officer, criminal, or terrorist? From airport and hotel safety to what to do in a hostage situation, this video tells you everything you need to know before you go! Produced by the Defense Intelligence Agency.

D*I*C*E 2001

This is a counterintelligence threat briefing you will never forget! Our very own Ray Semko (The D*I*C*E Man) will alert you to the latest unclassified threat information in an entertaining and informative fashion. This 37-minute version of Ray's famous Defensive Information to Counter Espionage (D*I*C*E) briefing is a must-see for anyone in the business of protecting the security of the United States. Produced by the Interagency OPSEC Support Staff (IOSS).

In The Public Domain

Do you know what procedures to follow if you want to publish in the open press? Do you understand what could happen if procedures aren't followed? In this segment, a scientist and would-be author wrestles with the issues and comes perilously close to giving away U.S. technological information to foreign interests. Produced by the NRO.

Web Content Vulnerabilities

U.S. Air Force Major James Lyons of the DoD's Joint Web Risk Assessment Cell (JWRAC) offers important tips to anyone involved in posting information to the Internet. His common-sense approach to web security offers solutions for protecting classified or unclassified, but critical information, from inadvertently falling into the hands of the adversary. Produced by the IOSS.

Order "Awareness 2001" by sending an e-mail to ioss@radium.ncsc.mil or send a FAX to (301) 982-2913.

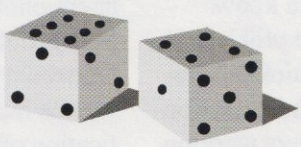
Director's Message

Spring Forward with OPSEC Awareness

I would like to extend my sincere appreciation to our good friends at the Department of Energy (DOE), Nevada OPSEC Program Office who hosted the 2nd Annual Regional Threat Symposium held February 6-7, 2001 at the DOE Nevada facility. It was at the suggestion of Kurt Haase and Wayne Morris, DOE Nevada, that the IOSS began offering a threat symposium for our West Coast customers similar to the 12-year running National Threat Symposium. This event had such strong attendance and participation (a 25% increase from last year), that it will now be one of the regular annual IOSS symposia.

On the previous page you see the announcement for the IOSS' brand new product, "Awareness 2001, A Security, Counterintelligence, and OPSEC Update" video presentation. This video, the first of its kind, was produced specifically to help those of you who have the responsibility to present annual security education and awareness training. It is our intention to produce an awareness video presentation like this one each year. We will feature timely information of vital importance to the entire national security community population. The IOSS will canvas the community each year and seek out current topics of interest and concern. We will be looking for your feedback both on the format of this new product and what topics you would like to see addressed next year. I would like to congratulate our own Lynne Yates for taking on this project, writing the script and taking it to completion. She enlisted the technical help from NSA's Information Assurance, Corporate Communications Productions, obtained approval from the National Reconnaissance Office and the Defense Intelligence Agency to include some of their outstanding video productions and has ensured that the marketing of the video gets maximum visibility.

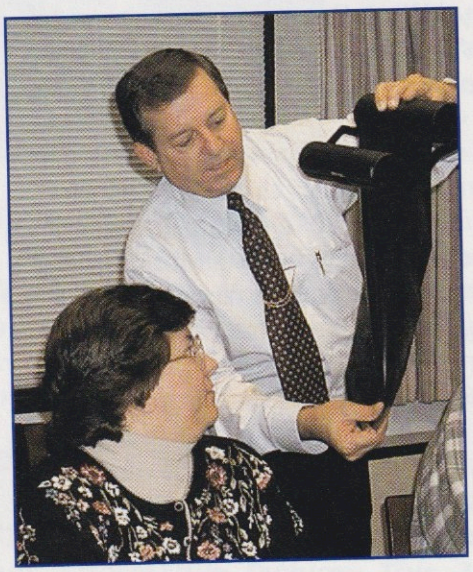
In closing, don't forget that the National OPSEC Conference and Exhibition coming up in June is ***your*** *event. Attending it ensures that you are engaged in your profession and that you have equipped yourself with the current information, products, and services you need to satisfy your customers. The IOSS and the OPSEC Professionals Society staffs work year round to make this a real "event." We have been able to keep the price down again this year to make it the most affordable program available anywhere. Evening events have been added this year at the suggestion of last year's attendees in order to further the ability to network and strengthen associations and identify new resources. See you there!*



Cartridges in Popular FAX Machines Are Potential OPSEC Vulnerability

by Lynne Yates
IOSS Staff

On January 21, Mr. Joseph Hurston, President and Chief Executive Officer of Cartridge Source of America, Inc. (CSA) briefed members of the Interagency OPSEC Support Staff (IOSS) on the potential threat to U.S. government



Mr. Joseph Hurston shows IOSS members the problem with thermal transfer cartridges.

critical information from the improper disposal of thermal transfer cartridges. These cartridges can be found in FAX machines, high quality color printers, video printers, badging printers and labeling/bar coding printers. These printers are all commonly used throughout the U.S. government.

Hurston, who once worked as a missionary pilot in Haiti, initially opened CSA in Florida in 1994 to manufacture computer printer, FAX, and other cartridges for various U.S. government equipment. His company expanded rapidly and its primary customer has been the Kennedy Space Center in Cape Canaveral, FL and its contractors.

A Startling Find

In addition to providing toner cartridges, CSA also collects empty toner cartridges for recycling. It was during this process that CSA made an amazing discovery — thermal transfer FAX machines and certain high-end color printers, including badging machines, produced a potentially serious OPSEC problem — ***a negative image of every document printed is retained in the thermal transfer take-up roll.***

All an adversary would need to do is find a discarded roll and use these negative images to potentially access critical information. Not only are these film images perfectly readable, they can be made into exact duplicate copies of the originals.

Fortunately, no classified information appeared on the rolls. Appropriate security measures had already been in place at Kennedy for disposal of cartridges from classified machines.

An OPSEC Vulnerability

The question still remained for Hurston — just how much information *could* be retrieved from these cartridges and how potentially dangerous is this situation?

Hurston surmised that enough unclassified information was available on these cartridges to present an accurate picture of operations at Kennedy Space Center — information an adversary would definitely like to know.

He initially explained the problem to the highest levels at the National Aeronautics and Space Administration (NASA). He has since been working diligently with NASA security personnel, even going aboard the Space Shuttles to search for potential vulnerabilities and providing proactive countermeasures to protect the information in these machines.

Hurston was thoroughly impressed with how NASA handled the situation. There was no denial of a potential problem and no recriminations, just a straightforward investigation into the situation, invention of new policies, and implementation of countermeasures to prevent future vulnerabilites.

For his efforts, Hurston received a citation from Mr. Roy Bridges, Jr., Director of the Kennedy Space Center for his "outstanding contribution...in the identification of vulnerabilities regarding the protection of Administratively Controlled Information and the development of the proactive measures for equipment using thermal transfer technology."

The IOSS Plays A Role

Hurston realized that if the problem existed at Kennedy Space Center, it most likely existed elsewhere in the government.

One of his aerospace contractor security contacts suggested he get in touch with the Interagency OPSEC Support Staff in Greenbelt, MD. Hurston hoped that the IOSS would help get the word out to other government agencies about this widespread problem.

Hurston considers himself simply a concerned citizen who wants to have attention focused on this problem. If the problem is as widespread as Hurston surmises, then his company will be available to assist in the identification of vulnerable machines and the efficient destruction of the cartridges.

Procurement Made Easy

Hurston realizes that many government agencies and industrial and commercial firms are now in possession of numerous FAX machines, high quality color printers and badging machines using thermal transfer (also known as dye sublimation) technology. Agencies queried by Hurston were unaware of this threat to their critical information.

He speculates that the new and easier procurement procedures (ones that allow government employees to use government credit cards to purchase equipment under a certain dollar value) are certainly making it possible for government employees to unwittingly circumvent equipment tracking procedures.

Hurston defines the problem with the cartridges as follows:

♦negative images are retained on the thermal transfer take-up roll;

♦disposal of spent cartridges is not adequately controlled, safeguards are not in place;

♦unauthorized retrieval and possession of spent cartridges can result in compromise of critical information by adversaries;

♦security and procurement offices are largely unaware of the vulnerability;

♦machine usage (unclassified data) and cartridge disposal policies and procedures are either non-existent or do not cover vulnerability issues; and

♦the workplace utilizes many varieties of these machines. Identification of existing in-place vulnerable machines is not an easy task in large organizations.

Having identified these problems, Hurston offers several suggestions on how to eliminate these vulnerabilities. He believes that if these suggestions are implemented throughout the national defense and intelligence communities, the risk associated with thermal transfer cartridges will be significantly reduced.

Reducing the Risk

Hurston developed the following recommendations to reduce the risk of losing critical information:

♦advise the security and procurement offices of the vulnerability;

♦locate existing in-place vulnerable machines (quantify the problem);

♦create recognition procedures for procurement offices to identify vulnerable machines in regard to future acquisitions;

♦establish a controlled cartridge collection/recycling program;

♦create and develop policies and procedures governing procurement and usage and disposal of thermal transfer/dye sublimation cartridges; and

♦update computer security plans and contracts with appropriate policies and procedures.

For further information regarding the OPSEC vulnerabilities of thermal transfer cartridges, contact:

Mr. Joseph Hurston
Cartridge Source of America, Inc.
1427 Chaffee Drive, Suite 5
Titusville, Florida 32780
(321) 267-7726 or (888) 319-2500
or send a Fax to (321) 267-7353 or
E-mail to ***csainc@metrolink.net.*** ■

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.

(continued from page 1)

"No matter how hard they 'push,' the evidence they seek normally just isn't there to be found. When the case was leaked to the press and Congress entered the picture, it did so with the expectation that, where there is espionage, there must be proof of espionage. This assumption is not true for PRC espionage, however, so many of the subsequent developments of the case had to do with coping with Congress' false assumption.

An Irresistible Force

"So great were the expectations that I call them an irresistible force. In the Lee case, the investigators ended up caught in the middle, between an immovable object of PRC intelligence practices and an irresistible force of public expectations.

"What we tend to see in PRC intelligence operations is at its heart an East-meets-West clash of cultures. China has its own set of intelligence principles, and so the ideas behind its operations often don't fit into our own categories. China also has its own way of carrying out operations, and its operating style often seems sloppy to Western observers.

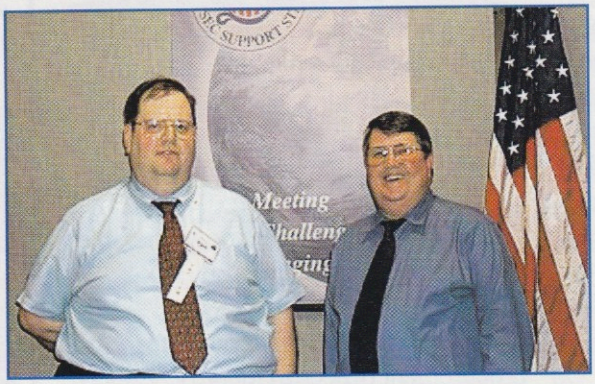
A Different Perspective

"When it comes to PRC sources and agents, we tend to think of intelligence operations as a process by which our adversaries steal information from us, but China tends to view the same situation as a process in which its friends give it needed information.

"The PRC tends to see its intelligence collection opportunities in terms of two preferred targets: visitors to China, and people who feel a sense of obligation to China and who thus can be subjected to a recruitment process.

"I think the important thing to remember is that, (although its reasons for doing so may be very complicated), in its intelligence operations, China does very simple things. It also tends to do the same things over and over, making it predictable.

For example, when China attempts to collect intelligence data from visitors to its country, it typically is much more active in certain places and in certain situations than in others.



Dr. Paul Moore and Mr. John Gaskill of the Centre for Counterintelligence Studies present a full-day training session for symposium participants.

Predictable Yet Effective

"The heart of its effort against visitors is to bring them into situations where there is a greater than normal chance that they may be indiscreet and mistakenly give up some information. Because it does the same things over and over, China is predictable.

"China's predictability makes it vulnerable to good OPSEC. The goal of good OPSEC against the PRC should be studying where and how the Chinese have collected critical information in the past and then cautioning visitors to avoid those situations, and studying the process the PRC has used in past recruitments in order to be able to warn targeted individuals that they may be at risk. The heart of the PRC's recruitment process is maintaining confidentiality, and the normal means of detecting the makings of a security problem is discovering that an employee has been withholding information or lying.

China's Intelligence Philosophy

"China's intelligence philosophy is much more concerned with exploiting its own strengths than its adversary's weaknesses. In most intelligence situations, China will avoid individuals with problems like greed or thirst for revenge.

"Instead, it focuses on finding individuals who believe they are doing good by helping China to modernize. Such individuals typically provide helpful information only a little bit at a time, though they may do so over a long time period."

Class reviews unclassified case studies with former FBI Agent John Gaskill.

M. Butterfly

The full-day training session also included discussions by Mr. John Gaskill, a retired FBI agent on how the Chinese have also used "traditional" methods of espionage in the past.

Among other topics, he discussed the details of the very bizarre Chinese-French espionage case of Bernard Boursicot, a French diplomat living in China who fell hopelessly in love with Shi Pei Pu, (a man disguised as a woman), on whom the Broadway musical *M. Butterfly* was based.

Gaskill related that, after forming a relationship based on a series of lies, Shi Pei Pu convinced Bernard Boursicot to spy for the Chinese. It was not until years later, when they were both arrested for espionage in France, that Boursicot learned the truth about his lover — that *she* was a *he*!

After the day's educational events, the DOE hosted an informal reception at the Texas Station for all of the participants to socialize and network with other individuals interested in operations security.

2001 — A D*I*C*E Odyssey

The second day was reserved for the classified sessions and it started off with the inimitable Ray Semko's presentation of "2001 - A D*I*C*E Odyssey."

Each year, Semko, aka The D*I*C*E Man (who is a member of the IOSS team), designs a new, entertaining and enlightening presentation that includes the latest threat information. At this session, Ray also unveiled his new "millennium" tuxedo designed to celebrate the the beginning of the new era.

Following "The D*I*C*E Man" was U.S. Army Lt. Col. James Stuteville from the Defense Intelligence Agency who offered new insights into the "Foreign Intelligence Threat." His classified briefing offered a Department of Defense perspective on this vital topic of interest and generated many questions from the symposium audience. Stuteville's in-depth knowledge of the topic assisted participants who had many questions on specific areas of interest.

Mr. Wayne Morris, Mr. August Schellhase, Mr. Tom Vaselopulos, and Ms. Cheryl Cirello at the DOE, Las Vegas worked tirelessly behind the scenes taking care of the security and technical requirements of the speakers and symposium attendees.

After lunch, an individual from the Central Intelligence Agency provided a fascinating discourse on Web Content Threats. His comprehensive briefing made everyone present painfully aware of the innumerable vulnerabilities to U.S. interests inherent in the Information Age.

This presentation led nicely into the next segment by Ms. Ruth Thomas, (also from the Centre for Counterintelligence Studies). Thomas focused on "Counterintelligence Implications of Personal Internet Information." Thomas' briefing was the only unclassified presentation of the day. Thomas demonstrated how effortless it is to acquire a wealth of personal information on any individual, with a minimum of cost, through the Internet.

She discussed how this information might be used by a hostile intelligence service for recruitment purposes. Thomas also offered practical advice on how individuals could protect their personal information from falling into the wrong hands via the Internet.

The final presentation of the symposium focused on "The Continuing SIGINT Threat." a representative of the National Security Agency provided unique and thorough information on this sensitive topic.

Critiques from the symposium praised the speakers and were uniformly enthusiastic about the location (Las Vegas) and the DOE facility. Many participants expressed gratitude for the opportunity to attend a seminar that was closer to the West Coast.

The next major IOSS event will be the National OPSEC Conference and Exhibition, June 11-15, 2001 in Tampa, Florida cosponsored by the OPSEC Professionals Society (OPS). See page 13 for a tentative schedule of events. ■

OPSEC Success Stories?

Log on to *www.ioss.gov!* Share your tale with the OPSEC community - tell us about your success using the 5-step process or help us all learn from your mistakes!

Protection of Critical Information Key to Success in Battle of the Bismark Sea

by Patrick D. Weadon
NSA Historian

The morning of March 3rd, 1943 dawned clear and bright on the Japanese convoy making its way through the Bismark Sea to the island of New Guinea. Sent from the massive naval complex at Rabaul, the group was composed of eight troop transports escorted by eight destroyers.

Its mission was to quickly transport more than 4,000 Japanese soldiers to the area around the town of Lae, on the northern New Guinea coast.

The officers and men aboard the ships hoped to be able to breathe new life into a planned Japanese offensive against renewed Allied attempts to control the region. Every man aboard realized that the battle for the island was at a crucial point, and that Japan desperately needed to regain the initiative or risk losing the battle for New Guinea.

The Beginning of the End

Almost from the moment General Douglas MacArthur arrived in Australia in February 1942 (after fleeing the Phillipines on the orders of President Roosevelt), he realized that the massive island of New Guinea would be the key to jumpstarting a massive counterattack against Japan in the Pacific Theater.

If the Allies could prevent Japanese forces from using the island as a staging area to attack Australia, it would be difficult if not impossible for Tojo and his compatriots to deal any kind of finishing blow to MacArthur's efforts.

If, on the other hand, Japan could wrest control of the island, and more importantly the sea lanes in and around the region, Australia and the Allied forces in the area would be in grave danger. Not only would Japan be able to attack major population centers in Australia, they would also be able to shore up the Empire's southern flank in such a manner that a herculean effort would be required to prevent the region from falling within the boundaries of the "Japanese Empire's Greater East Asia Co-Prosperity Sphere."

The effort to reinforce the surrounding area was a last desperate effort to try to win back the island of New Guinea for Japan.

In January 1942, the crucial town of Buna had fallen to the Allies. Now it appeared that General MacArthur's forces would have an opportunity to drive the remaining enemy forces into the sea.

The Green War

This was not good news for the Australian and American troops on New Guinea who had fought so hard to bring the battle at Buna to a decisive end. The island of New Guinea was in short, a hellish place. Brigadier General Pat Casey, an advisor to MacArthur at the time, noted that "he didn't see how human beings could live there, much less fight there."

William Manchester, in his book, *American Caesar* describes the conditions faced by the men who fought in what Manchester describes as "The Green War."

Manchester states:

"It wasn't until they (the soldiers) landed and ventured into the rain forests on steep, slippery root-tangled trails that the full horror of life there...struck them. Blades of grass seven feet high could lay a man's hand open as quickly as a scalpel. The jungle was studded with mangrove swamps, thick clumps of bamboo, and palms. Often, the trail was covered with waist-deep slop. The air reeked with vile odors — the stench of rotting undergrowth of stink lilies...when the rain stopped and the sun appeared, vast suffering waves of steam rose from the dank marshes...bugs were everywhere ... pythons and crocodiles lurked in the bogs...for every man suffering from a gunshot wound, five were laid low with illness...no one was hospitalized unless his fever rose above 102."

In short, the longer the fight for New Guinea took, the longer these brave men had to endure these horrible conditions.

Bushwhacked

Thankfully, the massive convoy that carried Japan's last hopes for winning the island for their Emperor would never reach Lae. Unknown to the Japanese command, the combined efforts of Allied codebreaking units had intercepted critical information on the convoy's intentions and had informed MacArthur's command of their coming.

Seizing the opportunity, MacArthur ordered General George Kenney, his air operations chief, to attack the force as soon as possible. Kenney, whose air exploits would make him a legend in the Army Air Corps by war's end, went to work in his usual style.

Due to the outstanding intelligence provided, the convoy was not hard to find. On the morning of the 13th, waves of American B-17 bombers

descended on the enemy ships and transports.

Kenney used the opportunity to employ a new technique in the attack that would come to be known as skip bombing, (which, as the name implies, involves literally skipping the attack bombs over the water, as you would a flat stone).

The attack brought a quick end to Japan's hopes of reinforcing Lae. All eight of the troop transports were destroyed, as well as four of the destroyers that had been sent to escort the group.

By March 5th, the only thing left of the convoy was 800 Japanese soldiers desperately trying to swim to shore.

Once again, the ability of the Allies to discover the enemy's plan while protecting their own, played a key role in winning the fight.

End Game

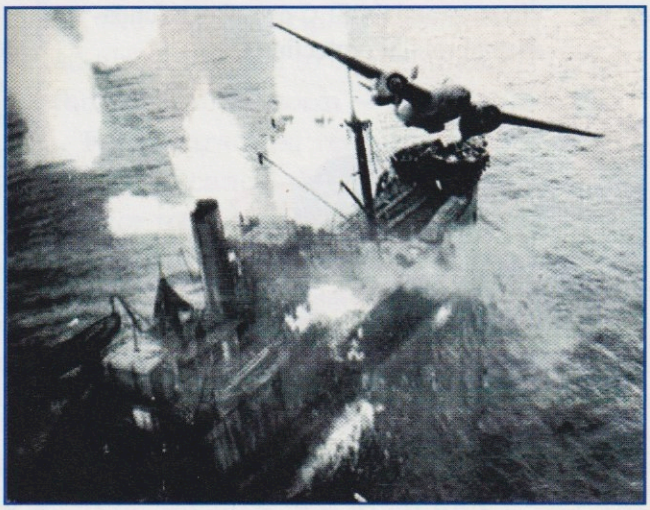
What are we to learn from the Battle of the Bismark Sea? What were some of the results that flowed from the outstanding work done by the intrepid codebreakers and skilled American pilots?

From a strategic point of view, MacArthur was able to have confidence that the battle for New Guinea would soon come to a close. President Roosevelt, General Marshall and a host of other policymakers in Washington, while focused mainly on the Third Reich, began to have increased hope that the fight in the Pacific might be turning their way.

For our purposes, however, the important point is that the many battle-weary troops on New Guinea lived to fight another day—and for the moment, avoided having to fight in the brutal conditions described earlier.

Not Just For Generals

Operations Security has always played a vital role in protecting our intelligence assets. It has been proven effective in protecting our Nation's security while promoting and preserving the lives of the many soldiers, sailors, airmen and marines in harm's way. ***In other words, OPSEC is not just for policymakers and generals.***



A Japanese transport is skip bombed during The Battle of Bismark Sea.

Operations security is important not only for the Commander-in-Chief and the generals at the Pentagon, but for those who are at the greatest risk of not coming back from a mission.

The Allies' Advantage

Harkening back to the noteworthy Battle of the Bismark Sea, think what might have happened if Japan had been aware of the fact that MacArthur's intelligence assets had detected a convoy. The force would have taken another route and it quite probably would have been the Allies who were bushwhacked.

It was fortunate that Japan, for the most part, considered the idea that the Allies were reading their codes an impossibility. Our ability to protect this precious asset was invaluable.

Conversely, Japan's inability to learn what the Allied side was up to afforded a tremendous advantage. To protect this precious secret, the commanders used every resource available to them, including OPSEC.

Countermeasures

The U.S. Navy was made painfully aware at Pearl Harbor that open, unclassified information provided the Japanese with the essential element needed to discover its vulnerabilities. After that disaster, active measures were undertaken to ensure that the enemy would be denied the information needed to mount a similar attack.

By 1943, America had effectively incorporated this lesson to its advantage. In addition to going to great pains on both the classified and unclassified levels to prevent critical information from leaking out, the Allies also used clever countermeasures to keep the enemy unaware of its sources and methods.

In the case of the Bismark Sea operation, a reconnaissance plane was sent out and told to fly close to the enemy ships so that they would assume the task force had been spotted. This, in turn, would lead the Japanese command to assume that the attack, which came on the heels of the sighting, was due to routine patrolling and not SIGINT or any other kind of intelligence operation.

The key point to remember, however, is that the necessary reinforcements never reached Lae—and those Japanese troops who did manage to swim ashore were in no condition to fight.

(continued on page 10)

(continued from page 9)

It is a cruel and harsh reality, but the hard work done in protecting the critical information ensured that, in March 1943, it would be Japanese soldiers who would die an untimely death, not Australian Diggers or American GIs.

Remember, when preaching OPSEC, that the wise and prodigious use of the 5-step process not only helps our Nation prevail against its adversaries, it sometimes determines who lives or dies.

Why We Fight

During World War II, Frank Capra, the renowned filmmaker, was asked by President Roosevelt to prepare a series of films entitled, "Why We Fight."

Their purpose was to remind the American people of what was at stake and to motivate them to do everything they could to contribute to the war effort.

Capra's goal was for Americans to realize that an Axis victory would not only be a disaster from a political perspective but that it would affect them personally.

Let *us* remember that the effective use of OPSEC will personally affect the lives of American service men and women who stand guard throughout the world. Their service and sacrifice has kept the peace and preserved American freedom. Their lives are precious — and OPSEC can play a fundamental role in protecting them. ■

OPSEC Fact

"Network system security is an ongoing concern for most businesses, but many companies are struggling to find the resources - financial and human - to deal with the growing number of threats that can bring down a company's technology infrastructure."

—"Cisco's Security Push," *Information Week*, September 2000

From the Editor

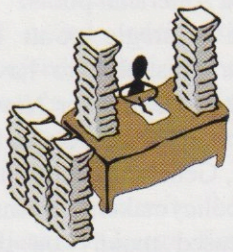
The winter months were very busy ones for the IOSS. I was fortunate enough to meet many *Indicator* readers in February at the Regional Threat Symposium in Las Vegas., Nevada and at a security awareness conference at the Defense Intelligence Agency (DIA) in March.

In addition to learning a great deal about the security challenges facing OPSEC professionals at those events, I was also informed by many attendees of their growing need for IOSS products and services.

The OPSEC community is growing in leaps and bounds and we have this newsletter as a forum to share information, so drop us a line!

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



Visit our website at www.ioss.gov

Snow Foolin' Folks - March East Coast Regional Symposium in Norfolk Cancelled Due to Forecast of Blizzard

It was an unprecedented and difficult situation for the IOSS — on the morning of Sunday, March 3, 2001, weather forecasters were predicting that a major snowstorm would blanket the entire east coast with potentially devastating consequences.

By 10:00 a.m., more than 60 of the 167 participants scheduled to attend our conference had already called to cancel their attendance due to the threat of the impending storm — and the calls were continuing to roll in. For contractual reasons, the IOSS was forced to make the decision to cancel the conference by 12 noon Sunday — 24 hours prior to the registration day.

It was definitely a gamble. If we had not cancelled, and the storm had been significant enough to close down the government, then other legal issues would have come into play. The demographics indicated that the majority of the registrants were traveling from the Washington Metropolitan area, with the worst of the storm supposed to hit the area just when they would have been on the road. Once the decision was rendered, we made every attempt to notify the participants of the cancellation.

As you may recall, the storm bypassed the area with only some sleet and freezing rain occurring on Monday morning, March 4. However, we still believe we made the correct decision based on the information available at the time.

We sincerely regret any inconvenience to our customers who were looking forward to an exciting week filled with excellent speakers and lively discussions - our only suggestion is - use those funds in June to come to the National OPSEC Conference and Exhibition in Tampa (see the following pages for details.) We guarantee — it won't be called off due to snow!

Tommy

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

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

To register online visit www.iaevents.com

Join us in Tampa!

The National Conference and Exhibition is fast approaching. We will be at a wonderful facility in Tampa. Speakers are working on dynamic presentations and the management staff is going all out to make the event an enjoyable one. A tentative schedule is listed below - ***the schedule may change*** due to last minute conflicts. One of the highlights will be the National OPSEC Awards Luncheon on Tuesday. If you haven't received a flyer in the mail, please call the IOSS or visit the website at www.ioss.gov for registration and up-to-date schedule information — or call the McNeil Technologies staff at (410) 553-6465 for additional information.■

Preliminary National OPSEC Conference and Exhibition 2001 Schedule

Monday — June 11, 2001 — Preconference Courses - Preregistration Required

	Salons I-K, L-N, O-Q	Stirling East	Salon VII-IX	Salon D-F	Edinburgh West
0900-1700	OP-300	Open Source Research	Computer Network Defense	Web Content Vulnerabilities	Counterintelligence
1130-1300	**Lunch in the Stirling Ballroom West and Edinburgh Ballroom East**				
1700-1830	IOSS Reception				

Tuesday — June 12, 2001 — Unclassified Sessions

Stirling Ballroom

0800 - 0820	Administrative Remarks
0820 - 0840	Opening Remarks from the Director NSA
0840 - 0930	Keynote Address

Edinburgh Ballroom

1000 - 1115	National OPSEC Awards Ceremony
1115-1200	Awards Luncheon Speaker
1200 - 1300	**Awards Luncheon**

	Stirling E	D-F	L-N	I-II & III-IV	VII-IX	X-XI
1300-1400	Counterterrorism	Marketing OPSEC	Force Protection	OPSEC Planning Workshops	Survey Planning Workshops	Program Development Team Workshop

Tuesday — June 12, 2001 — Continued

Time	Stirling E	D-F	L-N	O-Q	I- II & III-IV	VII-IX	X-XI
1415-1515	Threat Assessment	Professional. in Federal Govt.	OPSEC & Law Enforcement	Heat Transfer Technology	OPSEC Plan Workshops	Survey Planning Workshops	Program Develop Team Wkshop
1530-1700	10 Laws of OPSEC	Private Industry	Information Operations	Test Ranges			
1600-1900	Exhibits Set Up						
1700-1900	OPSEC Professionals Society Annual Meeting						

Wednesday — June 13, 2001 — Conference

0830-0930 **D*I*C*E 2001 — Edinburgh Ballroom**

Time	Edinburgh	Salon D-F	Salon I-K	Salon L-N	Salon O-Q
0945-1045	WWW Vulnerabilities	Marketing OPSEC	Professionalization in Federal Govt.	Heat Transfer Technology	
1100-1200	Terrorism and Foreign Visitors	Counterterrorism	Force Protection and Risk	Threat Assessment	OPSEC and Law Enforcement
1230 - 1330	**Lunch in the Stirling Ballroom**				
1330-1430	Information Operations	OPSEC Success Stories	Where the Rubber Meets the Road	Motivation Through Communications	Program Development Team Workshop
1445-1545	FOIA and the Web	Why Isn't Your OPSEC Program Working?			
1600-1700	Cyber Strategies	Program Ideas for A Small Organization			
1730-1930	Social Activity				

Thursday — June 14, 2001 — Conference

Time	Inverness A	Inverness B	Salon D-F	Salon L-N	Salon O-Q
0830-0930	Technology Targeting	Kosovo	Test Ranges	10 Laws of OPSEC	Private Industry
0945-1045	Imagery	The Legacy of Gunman	Program Ideas For A Small Org.	Cyber Strategies	Where the Rubber Meets the Road
1100-1200	Profile of A Spy	State Dept. Bugging	Why Your OPSEC Program Isn't Working	FOIA and the Web	
1200-1300	**Lunch in the Stirling Ballroom**				
1300-1400	Technology Targeting	Kosovo	Terrorism and Foreign Visits	Motivation Through Communication	Program Management Workshop
1415-1515	Imagery	The Legacy of Gunman	WWW Vulnerabilities		
1530-1630	Profile of A Spy	State Dept. Bugging			
1730-1930	Social Activity				

Friday — June 15, 2001 — Classified Sessions — Preregistration Required

Time	Inverness A	Inverness B	Salon I-K	Salon L-N	Salon O-Q
0800-1530	Threat Research	Communications Vulnerabilites	Analysis Tools	Program Management. Workshop *	Survey Planning Workshop *

*** Workshops - Morning Only - 0800-1130.**

Remember OPSEC When Posting to the Internet!

by Major Connie Wright, USAF

Army Staff Sergeant Robert Davis, a member of the U.S. Special Operations Command OPSEC Staff and a recent uate of the OPSEC Practitioner's Course, and his wife were searching the Internet for wise words about becoming nev ents again after 10 years. During the search, they discovered an interesting website that offered a wealth of good infc tion about the latest trends in baby care and parenting *and* it hosted message boards. They found an added benefit i message board specifically geared to military family members and friends. All together, the Davis family thought the found a great resource for baby advice. What a resource it might have been to the adversary!

While reading this message board, SSG Davis found his newly acquired OPSEC awareness alarm sounding. The he read, the more astonished he became while reading messages like the following **(with obvious OPSEC edits)** p on this Internet message board:

Hi all!

Well, Marty* gets back Wednesday after 10 days gone. Today is our anniversary. We plan to celebrate this weekend, but its still tough to be here without him. It's our first.

Also, big news today. I got an e-mail from him telling me that the ship is going unexpectedly on deployment in February!!! It is a —— deployment - for those of you not familiar with the FDNF (Forward Deployed Naval Forces) that is a LONG time. They are out SOOO much just doing regular ops, that they go on one —— per ——, as opposed to —— every —— like stateside ships. But not only that - he got orders to his new ship, the —— in ——, and they leave on deployment just —— after we arrive in —— for a FULL ——!!!

Needless to say I am not too thrilled. He'll be gone like —— of the next —— months. I guess there is some rule against that, but we do not want to upset his orders because we are so happy with the ship he got into, the ——. Oh well, it's the Navy life I guess!!! I am not blind to it as I was a Naval officer too, 'til just —— of this year, but who would have expected he'd be gone THIS much this coming year! Goodness gracious!

Okay, the good news - I hope to meet the ship in ——, ——, and ——. I met it when they went to the —— earlier this year (oh yes, did I mention he just got back from a ——month deployment in ——?

Anyway, all this means that we have to pack out by ——!!! I am floored! So much to get ready for in so little time and two weeks of that we are going to —— househunting. Goodness! I am sure we will be fine, but it is still a lot of news to have gotten in one day. Thanks for letting me share! You gals understand - that's what's great about this board!!!

God bless,
Carrie

*Names have been changed.

And this one:

Hello everyone!

In ——, my husband will be in ——. So, for my son's first Christmas and birthday, we're flying to the States.

In total, we will be travelling for —— hours. Here's the plan: leave at ——, get to —— airport at ——. We leave —— for —— at ——p.m. We have a —— hour layover, a 9-hour flight to —— and arrive just in time for rush hour.

It could be —— hours with an 11-month-old boy. Any tips VERY welcome!

Barb

Certainly, the second message doesn't contain as many mission-related OPSEC indicators, but it is indicative of the information innocently posted and readily available to any number of "bad guys" who might be inclined to look for it. This trend continued throughout the message board. With a simple click of a mouse, readers could find out the names of expectant mother and spouses, dates of birth, other children, assignment information, and any details the message writer wished to share.

The available information spanned services, ranks, and specialized assignment locations. For instance, one message board member informed readers that her husband works for the 742nd MI BN out of NSA! There's no telling who might key in on her particular posted messages.

On the other hand, the first message is filled with critical indicators. This prompted a concerned SSG Davis to contact the message board moderator to suggest that the posting might contain just a bit too much information. The moderator accepted his suggestion and pulled the message - a successful countermeasure. Yet, the amount of data posted on this message board, both operational and personal, remains significant.

This one website, discovered by accident, reveals a glimpse of an expanding problem — how to protect critical operational information in the Information Age. As recently as a decade ago, this type of OPSEC vulnerability was limited to highly sophisticated networks that could only be exploited by well-trained technicians. This is no longer the case. Now this particular threat can originate from a single person with a PC and access to the Internet — not very sophisticated and not very expensive, but just as significant to operational success or failure.

It's obvious that the intent of this message board is the honest exchange of thoughts and ideas. In reality, all the regulations and directives in the world can't stop normal communication, and no one would want to. Therefore, the only imaginable way to reduce the risk as this vulnerability increases is through training, awareness, and viable, dynamic OPSEC programs. ■

New Secretary of Defense Donald Rumsfeld Says America Faces New Vulnerabilities During Period of Continuing Change

Remarks taken from a speech delivered by Secretary of Defense Donald Rumsfeld , The Pentagon, Washington, DC , Friday, January 26, 2001.

"Distinguished guests, including many veterans who honor us by their presence. Men and women of the finest military in the world. Earlier today, I was in the White House with the President, and he asked me to deliver a message, a message to every one of you who wears our country's uniform, and to every civilian employee of the Department of Defense.

A Presidential Tribute

It reads: "To the Armed Forces of the United States and the men and women whose work supports them: Your service in the cause of freedom is both noble and extraordinary. Because of you, America is strong and the flame of freedom burns brighter than at any time in history.

Your country can never repay you for the sacrifices and hardships you endure, but we are grateful for the liberties we enjoy every day because of your service. As your Commander in Chief, I will always support you and your families so that this great Nation continues to have the greatest armed forces in the history of the world. Thank you. George W. Bush, President of the United States."

A New World

As General Shelton said, this is not my first tour of duty here. Since my last tour, a great deal has changed. Twenty-five years ago, Warsaw was the name of a military pact opposed to the ways of the West. Today Warsaw is the capital of a new member of NATO.

Twenty-five years ago, American freedom was menaced by the Soviet empire, and a wall cut not just Europe, but a world, in two. Today that empire is no more, the wall is down, and the Cold War is over.

Twenty-five years ago on this field, two old friends, Doc Cooke [Director, Washington Headquarters Services], and Andy Marshall were here at a similar ceremony. And today, well, they're here again. Some things just don't change.

The System Works

There's a story that dates back almost that far, to the early days of the Reagan presidency. A young GI on the front lines in Germany asked our ambassador there if he ever got to see the President. Our ambassador replied that sometimes he did.

"Well," the GI said, "you tell the President we're proud to be here and we ain't afraid of anybody." A few weeks later, the ambassador saw the President, and he passed along the GI's message. Not long after that, back in Germany, the GI was listening to Armed Forces Radio and the President's weekly radio address.

And when he heard Ronald Reagan tell the story of a message sent by a GI in Germany through our ambassador, the soldier ran out of the quarters, down through the company area, shouting, "The system works! The system works!"

On behalf of President Bush and Vice President Cheney, and the civilian and military leadership here in the Defense Department, I make this pledge today to every man and woman wearing a uniform. We will work to make the system work, work so that you can serve with pride and know that service to our Nation is a sacred calling, work so that America and her friends and allies are strong and secure, and work so that the cause of freedom will better bind the community of Nations seeking not conflict but common purpose.

President Bush takes office with three goals in mind: to strengthen the bond of trust with the American military, to protect the American people both from attack and threats of terror, and to build a military that takes advantage of the remarkable new technologies to confront the new threats of this century.

Mission and Mindset

Reaching those goals is a matter of mission and of mindset. Among the things we must combat is a sense that we have all the time in the world to get to the task that's at hand.

There's a sense out there that we can't or we needn't act, because the world is changing; that we're in a transition period between the Cold War and the next era, whatever it may be; and that we can wait until things shake out and settle down a bit.

But it seems to me that the state of change we see in our world may well be the new status quo. We may not be in the process of transition to something that will follow the Cold War.

Continuing Change

Rather, we may be in a period of continuing change, and if so, the sooner we wrap our heads around that fact, the sooner we can get about

the business of making this Nation and its citizens as safe and secure as they must be in our new national security environment.

We enjoy peace amid paradox. Yes, we're safer now from the threat of massive nuclear war than at any point since the dawn of the Atomic Age, and yet we're more vulnerable now to suitcase bombs, the cyber-terrorist, the raw and random violence of the outlaw regime.

Meeting the Threats

Make no mistake: keeping America safe in such a world is a challenge that's well within our reach, provided we work now and we work together to shape budgets, programs, strategies and force structure to meet the many threats we face and those that are emerging, and also to meet the opportunities we're offered to contribute to peace, stability and freedom.

But the changes we make in our defense posture, the innovations we introduce, take time to be made part of a great military force. We need to get about the business of making these changes now in order to remain strong, not just in this decade, but in decades to come.

But today really isn't the day to speak of budgets, programs or policy. That will come soon enough. It's a day to renew our promise, the debt we owe the people who serve.

The President and I believe the men and women who freely elect to wear the country's uniforms deserve not only our respect but our support, and yes, our appreciation. And the men and women who serve this country in times of conflict deserve not only our thanks for their sacrifice, but our commitment to value every veteran.

To the proud professionals here today and around the world, let me remind us all, this department does not stand alone. We will work with the diplomatic community and the intelligence community, to arm our President with the options and the information and capabilities needed to defend American interests and to pursue every avenue to keep the peace.

I know, for my part, as I work each day with the enormously talented men and women the President has fashioned in his national security team, that we are members of the same team, serving the same end, committed to pooling our strengths and serving our President and our Nation.

The President and Vice President Dick Cheney, Colin Powell, [National Security Advisor] Condi Rice, [Director of Central Intelligence] George Tenet—no one could ask for a finer group of colleagues in this critical mission.

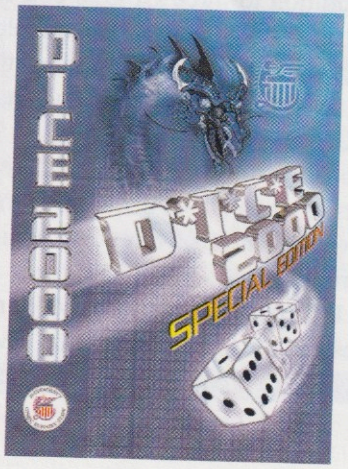
The Ultimate Safeguard

I close with a thought that occurred to me as President Bush spoke on Saturday at the west front of the Capitol about the qualities that make America special and exceptional.

He talked about civility, courage, character—reminders that the strength that matters most is not the strength of arms, but the strength of character; character expressed in service to something larger than ourselves.

And if that is an ultimate safeguard, then we indeed are a Nation blessed. One cannot stand where I now stand, one cannot look out at Arlington's row on row of headstones, without being powerfully reminded that the spirit of service and sacrifice still lives in this country. So my thanks to each of you for this welcome, and for sharing this ceremony today.

I accept the charge the President has placed on me with a sense of honor. I welcome this reassociation with the men and women of the American military—Active, Guard and Reserve—who put service above self and country above all. Thank you very much." ■



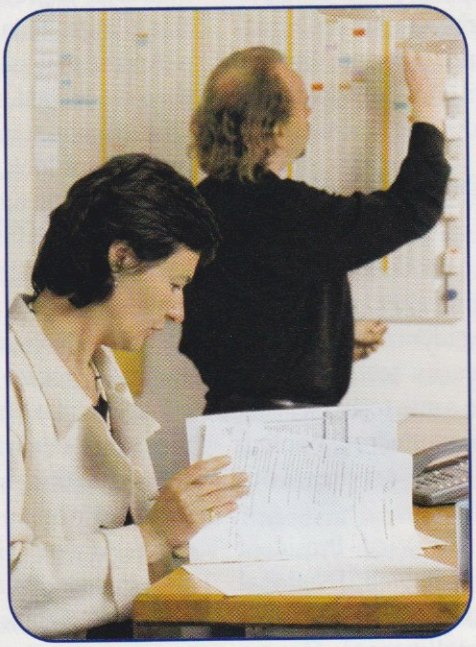
The IOSS is still accepting orders for the IOSS video, "D*I*C*E 2000, Special Edition." Order by sending an e-mail to ioss@radium.ncsc.mil or send a FAX to (301) 982-2913.

Training OPSEC Managers and Working Groups - At the IOSS and On the Road

by John Glorioso
PDT Manager

In January 2001, the Program Development Team (PDT) of the Interagency OPSEC Support Staff (IOSS), offered a new training program, OP-390 (Program Development for OPSEC Managers), to the OPSEC community.

The PDT had to overcome a blizzard, a newly revised instructional program, and some minor modifications to the original OP-390 course, but the program was successful and provided excellent insight into the direction of this new instructional course.



The PDT was very fortunate to have so many intelligent and energetic students in attendance for the first offering of the new OP-390.

The synergy that developed between the trainers and their colleagues in the class fostered productive dialogue and produced valuable input to assist the PDT in making adjustments to the course for future offerings.

While the PDT was teaching the instructional program, additional fine-tuning took place. In retrospect, the course didn't change drastically from its original design, but the minor modifications that were made seemed to have strengthened the overall course material. Participant feedback indicated that the changes were on the mark.

Proper Alignment

The introduction of a training program designed and developed exclusively for OPSEC managers and coordinators achieved one of the goals of Mr. Tom Mauriello, Director of the IOSS.

Those who are ardent readers of *The OPSEC Indicator* may recall articles in a past editions wherein Mr. Mauriello emphasized the importance of working diligently and decisively in order to incorporate OPSEC into organizational operations, programs and missions.

The IOSS is confident that the revised OP-390 course will provide the new OPSEC manager with an understanding of how to get a new OPSEC program off the ground. It will also definitely aid a current OPSEC manager by offering perspectives on what can be done to revitalize a dormant OPSEC program.

Community Interest

When the PDT initiated the new program, we anticipated a strong interest from the OPSEC community in attending courses at the IOSS. However, we were very surprised when we began to receive numerous requests from OPSEC managers to transport the OP-390 to their site and inquiries whether the training program could include their entire OPSEC working groups.

Our initial expectations of "a strong interest" had to be reclassified as "an unprecedented interest." The PDT was extremely pleased; the increased interest in the course reinforced our belief that the program was needed. At the same time, this proved to be a daunting challenge.

The request to include the OPSEC working groups in a class designed primarily for managers, might have been difficult to pull off. However, the team accepted this instructional obstacle with enthusiasm and a strong commitment to meet the challenge.

It was eventually decided to present the course exactly as it was. We realized that those selected to work in an OPSEC working group would require the same information and classroom exercises regarding organizational matters as the OPSEC managers in the development of a new program.

On the Road Again

In addition to three OP-390 courses offered at the IOSS, the PDT traveled to eight work sites, delivering the course to OPSEC managers and their OPSEC working groups.

Included in the site and organizational visits to teach OP-390 were five military organizations, three of which were multiorganizational in nature.

The U.S. Air Force hosted two of the courses and the U.S. Coast Guard invited the PDT to present OP-390 at one of

their sites.

In addition to the military training, the IOSS worked with the Department of Energy (which already has an established OPSEC program) in developing a new OPSEC program at one of their locations. The PDT also delivered the training program to the Boeing Corporation, a government contractor, that maintains a vigorous OPSEC program and has very knowledgeable OPSEC coordinators.

The Boeing Corporation teaching venture gave the PDT insight into the world of private industry, one that faces many of the same concerns as government agencies in addition to problems unique to the corporate world.

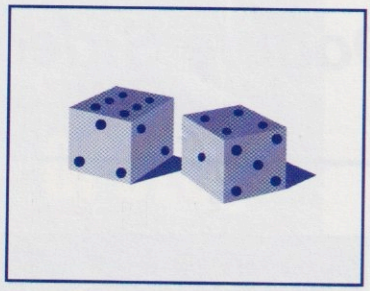
Consultations

As you may already know, the PDT exists to provide assistance wherever we can in your future OPSEC endeavors. If you wish to inquire into the feasibility of having OP-390 taught at your site, or would like an OPSEC program assessment or program consultation, call the Program Manager, Mr. John Glorioso at 301-507-6232 or e-mail him at jglorio@ radium.ncsc.mil.

A Special Thanks

The Program Development Team would like to thank everyone who attended our OP-390 classes at the IOSS and on the road. The PDT has benefited from working with each and every one of you.

You offered us a chance to work with very dedicated individuals who were open and honest as ideas were exchanged. All of us on the The Program Development Team sincerely hope that we assisted you in the task of creating and promoting your own OPSEC programs.■



Upcoming Training Courses and Symposia

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

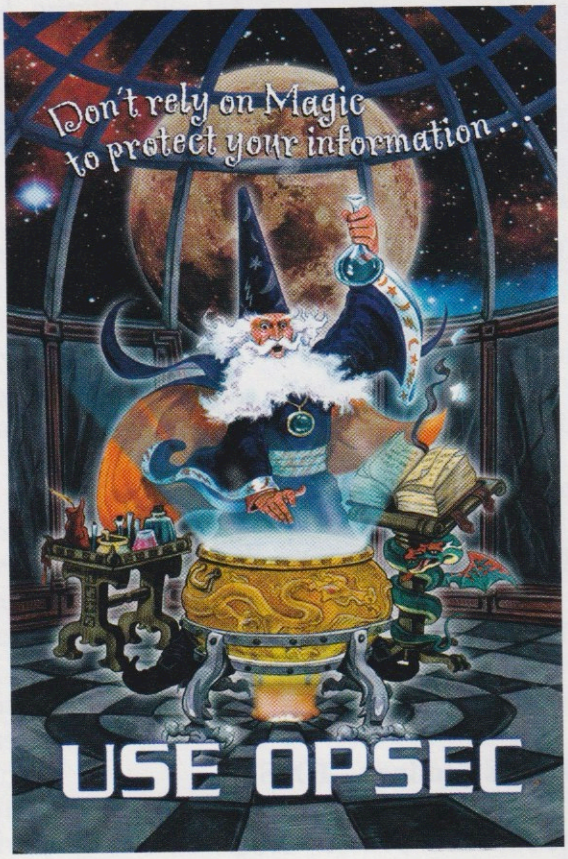
21-23 August—Web Content Vulnerabilities Seminar—IOSS

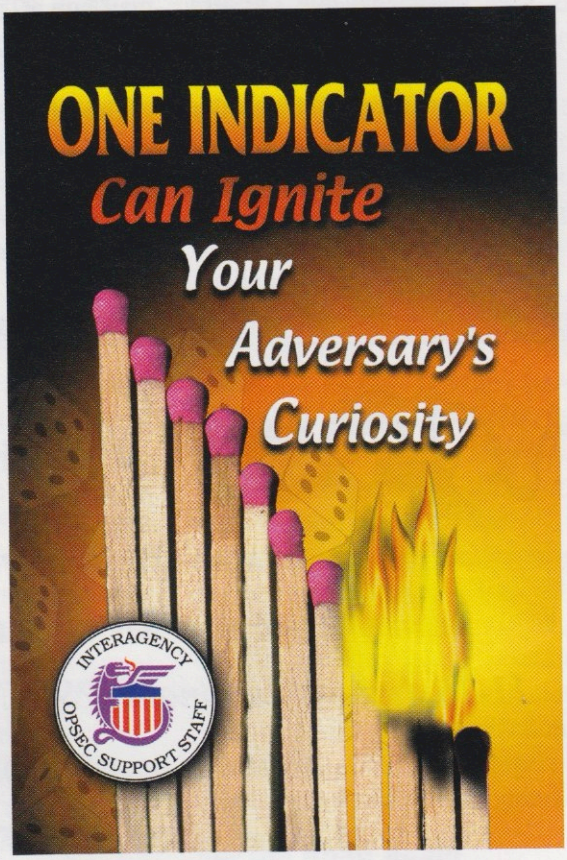
10-14 September—OP-380, OPSEC Practitioner's Course—NCS

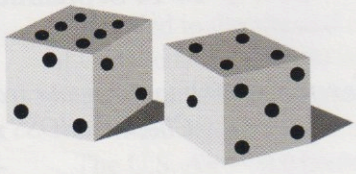
We are currently putting together our training calendar for the next fiscal year which will be mailed out this summer. Check the IOSS web page for the most current list of course offerings.

NEW OPSEC POSTER

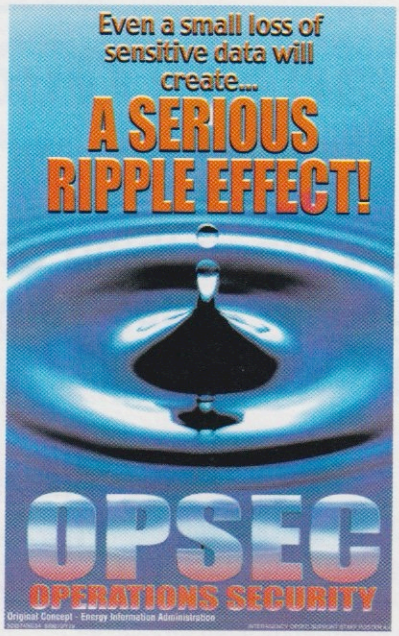
Poster #4 (Double Sided)







Poster #3 (Double Sided)



NAME (Mr./Mrs./Ms./Rank): _____

AGENCY/ORGANIZATION: _____

IF CONTRACTOR, NAME OF SPONSORING ORG: _____

POSITION/TITLE: _____

MAILING ADDRESS - Business: _____
Street Address/P.O. Box: _____
City/State/Zip Code: _____

Commercial Phone: _____
Commercial Fax: _____
E-mail Address: _____

Would you like to be added to the IOSS mailing list? _____

Poster #(s) _____
Quantity _____

Please complete and mail to
Interagency OPSEC Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
or
Send a Fax to (301) 982-2913

ORDER FORM FOR OPSEC POSTERS

Quarterly Quote

"It's a funny thing about life, if you refuse to accept anything but the very best you will very often get it."

— W. Somerset Maugham
1874-1965
British Novelist and Dramatist

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