Newsletter of the
OPSEC Professionals Society
ENABLING CRITICAL INFORMATION IDENTIFICATION, VULNERABILITY, ANALYSIS & RISK MANAGEMENT

The Operations Security Professionals Society, P. O. Box 150515, Alexandria, VA 22315-0515 www.OPSECSociety.org
Volume 1, Issue 6, September 2013

President's Message

by Valerie Simpson, OCP

Hi Folks,

I hope everyone had a good summer and a safe one at that. As your new president, I'd like you to know that my first crack in serving OPS was chairing the Communications Committee. A few years later I served as your Vice President as well as Chairman of the Awards Committee. Together with committee members, we developed the "Sam Fischer Award for Operations Security Excellence." We intend to issue the first award in 2014. Please take a look at our web site for more information and so that you can start developing your award package now. Be sure to follow instructions and if you have any questions by all means feel free to contact the Awards Committee who will be able to clarify any questions you may have regarding this prestigious award and its criteria.

2013 turned out to be a challenging year with budget cuts across the government which ultimately affected the IOSS. Because of this, the IOSS will no longer be hosting the National OPSEC Conference (NOC) and OPS is going to attempt to fill the void. To support this endeavor we formed the Conference Exploratory Committee. We'll need a lot of support to pull this off so if you are interested please contact Dan Phillips at (360) 396-5345 or via e-mail at secretary@opsecsociety.org. If you're unable to help out please spread the word.

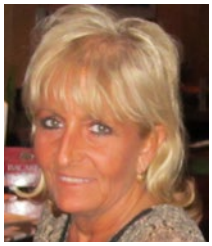
The ultimate goal of OPS continues to be promoting best practices while reducing vulnerabilities to your various government, industry and corporate missions. Terrorism continues to this day and will never end. Because of this we need more than ever to keep OPSEC at the forefront, so that we don't lose sight of it because together we "CAN" do it!

As your newly elected president I take great pride in this appointment and know that I can't do it alone. If you would like to assist the Society in any capacity please let us know. You can be - more than just a "member." We have numerous committees all of which need help. More importantly, it is crucial that the NOC continues. After all the years there was a NOC we can't let it stop now.

In closing, let's continue to work together to make this a safer country in which to live, and as I always say "If your eyes are closed – you can't see what you can't see."

Sincerely,

Valerie Simpson, OCP
16th National President
OPSEC Professionals Society
president@opesecsociety.org
www.opsecsociety.org



Inside This Issue

OPS NEWS

OPS Participates in Redstone Arsenal OPSEC Day

The Missile Defense Agency in conjunction with US Army Garrison Redstone Arsenal, NASA's Marshall Space Flight Center and other agencies conducted the first ever OPSEC day at Redstone Arsenal in Huntsville, Alabama on 20 August 2013. Over 150 attendees including many military and federal civilian OPSEC managers and security managers, and contractor facility security officers participated in the daylong conference. The conference drew a lot of attention and proved to be great success, paving the way for future annual OPSEC events at Redstone Arsenal. OPS Board Member Greg Hoffman, MDA's OPSEC Program Manager, served as the event coordinator and master of ceremonies. National Secretary Dan Phillips, OCP, represented OPS and participated in a panel discussion at the end of the day. Additionally, OPS donated logo items and a free membership for the raffle held during the conference.

New OPSEC Certified Professional

New OPS member Scott Dobravolsky, OPS National Secretary Dan Phillips, OCP and Board Member Greg Hoffman at the OPS table at the Redstone Arsenal OPSEC day.

New OPSEC Certified Professional

Congratulations to Jonathan (Jon) Herrmann, OCP, Senior Information Operations Analyst for 1st IO Command, U.S. Army OSE.

Follow OPS on

LinkedIn

New Corporate member

OPS is proud to welcome EM Solutions as a new corporate member.

EMSolutions

as a Bronze level member

http://www.emsolutionsinc.com/About-Us.aspx

Our other Corporate member

FE&E

Financial Examinations & Evaluations, Inc.

CLARITY FROM COMPLEXITY

The OPSEC Professional Society is a Proud Sponsor of

Lint Center™

for National Security Studies, Inc.

EMPOWER, ENHANCE, ENABLE

"OPSEC in my own words"

by Rick Bowser, MSCoE OPSEC Program Manager
IOC, SPTMS

Plagiarize – to steal and pass off (the idea or words of another) as one's own. There's obviously the wrong time to do that, such as school reports, hit song, or some scientific breakthrough. This can get you kicked out of school, sued, or discredited. However, plagiarism is used and highly recommended in several venues where it will save time and help prevent the reinvention of the wheel. If you have a great OPSEC idea or document, then share it and help other OPSEC Officers streamline their program and save some time. Although not always innovative, I do get a little creative and see OPSEC potential from other people's ideas. Unfortunately these seem to require permissions and license agreements. This can be a frustrating and lengthy process, but can result in great dividends for your OPSEC program. I currently have a license agreement with FX to use a short segment from the Sons of Anarchy portraying the vulnerabilities of cell phones. I'm currently working two other issues through Experience Hendrix, LLC, for a poster and AMC Film Holdings, LLC, for a short clip from The Walking Dead. The first step is seeing something that can be used, normally as an awareness product in the form of a poster or during your briefings. Next you need to determine who owns that product and try to find an address for their legal representatives. I'll send a letter outlining my desire for the use of their product to that address and await (patiently) a response. This can take several weeks to several months. If I don't hear back from them, then I send another letter or I check to see if I can locate a telephone number and actually talk to someone or get a name of someone who handles license agreements. If I can talk to someone and get my foot in the door, I can determine if there is any interest, express my idea(s), and let them know that my (Ft Leonard Wood's) contracting office and legal representatives will be in touch. Once the contracting and legal folks review a draft license agreement (either FLW's or theirs) then it's a waiting process until an agreement can be reached, or not. If it's approved, then you can create a "no cost" purchase requisition (PR), if no cost is associated with it, or if your program/installation has available funding, then you still have to create a PR. The PR goes to your contracting office and is subsequently awarded. As mentioned earlier, this is a frustrating and painstaking process, but grab on like a tenacious pit bull and don't let go!

Sequester And Furloughs: It's Discount Espionage Time

Homeland Security Today, July 15, 2013

by James Lint and Timothy W. Coleman

http://www.hstoday.us/blogs/guest-commentaries/blog/sequester-and-furloughs-its-discount-espionage-time/ce7c3324c8fc03c57cac45bacd507b1a.html

On his deathbed in 1801, legend has it that the infamous American Continental Army Gen. Benedict Arnold, a hero of the battles of Ticonderoga and Saratoga who defected to the British Army, uttered his regret: "Let me die in this old uniform in which I fought my battles. May God forgive me for ever having put on another."

But while scholars have debated the prevailing historical wisdom that Arnold's treasonous conversion was motivated by his frustration at having been passed over for promotion and outraged that others took credit for his achievements and military victories, a congressional investigation indicted his motivation was purely financial -- he was nearly penniless, having spent much of his own money on the American war effort. But when he joined the British Army as a brigadier general, the Red Coats gave him what was then a very generous pension and a £6,000 signing bonus.

It's a familiar story, though: money, or ideology; sometimes both.

For American traitor Navy communications officer John Walker, Jr., his motivation for nearly two-decades of spying for the Soviets (which included providing "enough code-data information to alter significantly the balance of power between Russia and the United States"), was purely financial, prosecutors said.

Heavily in debt and bitter that his brilliance had gone unrecognized, veteran CIA Soviet counterintelligence officer Aldrich Ames -- among other things -- sold to the KGB the identities of the CIA's agents secreted throughout the Soviet spy agency.

FBI Soviet counterintelligence agent Robert Hanssen spied for Soviet, and then Russian, intelligence services for 22 years also partly due to the same frustrations that tormented Ames, but also partly, it seemed according to prosecutors, because of the tastes of an expensive mistress. The Justice Department's Commission for the Review of FBI Security Programs said Hanssen "possibly [was] the worst intelligence disaster in US history."

While these turncoats spied against their country during an espionage boom when the Soviet's were quite willing to cut CEO-equivalent paychecks for such big fish, they were the exceptions rather than the rule. In today's austere espionage market economy, brought on by sequester and furloughs, foreign intelligence services are far more likely to ensnare a broke and bitter GG-13 with access to secrets for a bargain basement price.

Foreign Intelligence Security Services (FISS) still keep a keen eye out for the Walkers, Ames, and Hanssens, but they're also spending a great deal more time assessing the vulnerabilities of the many lower level military and Intelligence Community (IC) employees who have access to valuable secrets.

For decades, the US military, IC and contractors have been required to not only continuously evaluate their workforces for eligibility to access classified information, but also to be on the lookout for signs and indicators of potentially treasonous espionage from within their ranks. This includes the criminal leaking under the nation's espionage laws of the nation's most closely guarded foreign intelligence collection operations -- -- espionage operations former National Security Agency (NSA) and CIA director, AF Gen. (Ret.) Michael Hayden, recently pointed out that all nations' intelligence services engage in.

Consequently, the failure of the early warning system to alert what NSA contractor Edward Snowden was up to has provoked an intensive investigation into whether there were, in fact, signs and indicators that someone had observed that weren't properly reported. Former NSA official John R. Schindler recently remarked that Snowden's security clearance background investigation was "clearly flawed."

The threat of penetration by FISS is ever-present, and the Army trains its soldiers as well as civilian employees to always be vigilant. Training and awareness efforts are clearly articulated under US Army Regulation 382-12, Threat Awareness and Reporting Program (TARP), revised by the US Army on Oct. 4, 2010.

Formerly known as Subversion and Espionage Directed Against the US Army (SAEDA), TARP outlines the policy and responsibilities for threat awareness and reporting within the US Army. Specifically, it requires Department of the Army (DA) personnel to report any information to counterintelligence offices regarding known or suspected espionage, international terrorism, sabotage, subversion, theft or illegal diversion of military technology, information systems intrusions and unauthorized disclosure of classified information, among other required security and espionage concerns.

As the revised directive states: "The primary focus of this regulation is to ensure that DA personnel understand and report potential threats by foreign intelligence and international terrorists to the Army. Threat awareness and education training is designed to ensure that DA personnel recognize and report incidents and indicators of attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against the Army and its personnel, facilities, resources and activities; indicators of potential terrorist associated insider threats; illegal diversion of military technology; unauthorized intrusions into automated information systems; unauthorized disclosure of classified information; and indicators of other incidents that may indicate foreign intelligence or international terrorism targeting of the Army.

Following the digital data dump of roughly a quarter-million State Department cables -- six percent of which were classified "Secret" and the rest were either "Confidential" or unclassified -- accessed via classified Internet networks and downloaded onto thumb drives by low-level, but sufficiently cleared 23-year-old Army intelligence analyst, Private First Class Bradley Manning, President Obama on October 07, 2011, issued Executive Order 13587 that required government-wide "structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information."

The order applies to "all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks …"

All of these security efforts are not without justifiable reasons. Cleared personnel can become the target for recruitment by foreign spies and hostile intelligence services by no fault of their own. It is simply the reality and consequence of having access to classified information and sensitive US government secrets.

Not access alone

It is not only access to classified information that makes one an inviting target, however, there are other activities that increase the desirability. In fact, any Army team member/employee and or soldier can be targeted because of where they are stationed, where they travel or even because of an ethnic or cultural background of particular interest.

It should be noted and emphasized that being a target for recruitment does not necessarily reflect poorly on an individual. The opposite also applies, especially if the reason a specific person is targeted is because of his or her susceptibility to recruitment or exposure to compromise. Even so, just being a target does carry with it embedded risk factors, as it clearly increases the potentiality that a weakness or pressure point can be discovered and exploited by foreign intelligence collectors.

Targets of convenient opportunity

The historical record clearly demonstrates that US personnel with security clearances are regularly targeted. 'By hook or by crook,' foreign counter-intelligence agents have repeatedly been able to entice Americans to commit treason. The question then quickly becomes, what is it that makes America and would-be patriots such inviting targets of opportunity?

Prominent and well-publicized instances of Americans turned traitors shows that monetary reward and financial gain are very often a major driving factor in the equation. In turn, it should come as no surprise that foreign intelligence agents seeking new, well-placed assets often examine the financial circumstances and standing of identified potential targets.

Financial difficulties provides an initial and eventually lucrative ingress of potential exploitable temptation to facilitate the evolution of an individual's compromise – and eventual treason. But it is generally not the only factor that's in play in the targeting and recruitment effort.

Win, place or show: An espionage trifecta

Another and sometimes more nefarious element to recruitment can include exploiting personal feelings of disillusionment, anger, frustration and disappointment. These emotions can exist for a multitude of reasons, and can run the gamut from being passed over for a promotion, feeling underappreciated at work, disgruntled with the Army … or even America itself. These beliefs -- indications of which can openly manifest as attitudes of anger and resentment -- are recognized by foreign intelligence services' case officers as openings to manipulate a potential target into justifying his or her espionage.

This can all add up to a desired trifecta of opportunity for a foreign counterintelligence case officer – a potent, readily exploitable human Petri dish seething with psychological, financial and other stressors that make the person a target ripe for recruitment.

An individual who possesses a security clearance, has financial problems and is disgruntled poses a dangerous triad … and a compounding problem for counter-

intelligence interdiction efforts. In the end, a counterintelligence target that embodies the aforementioned trifecta is one that has two more levers to pull, and two more pressure points than is required for an FISS to target.

This trifecta, in essence, can define the elements required for the low-hanging fruit of an American traitor that's ripe for the picking.

Catch more flies with honey

With the current budgetary environment, furloughs the talk of the town, and sequestration the topic of water cooler chatter, low-hanging fruit that bear the elements of trifecta targets are sure to abound. Just a superficial reading of "Letters to the Editor" in various magazines and publications widely read by federal employees and members of the military makes the case for a target-rich environment for foreign agents. The problem is compounded by a growing segment of government personnel -- many of whom likely hold security clearances -- venting their frustration and anger in Internet blog comments, making them identifiable potential targets for recruitment.

Disgruntled individuals that publicly voice their justifiable concerns make easy work for foreign intelligence operatives who seek potential turncoats of opportunity. In many respects, it would appear as though potential opportunities for penetration are being served up on a silver platter at an all you can eat buffet where the chow line stretches around the proverbial corner!

We could even say that we are ensuring job advancement prospects for foreign intelligence agents and providing the very fodder for enemy promotions with such a perfect storm for motivating espionage from within our own ranks.

Consequences of context

Currently, sequester and current furloughs are expected to impact soldiers with great effect. Stress and greater work scrutiny, coupled to an increase in regulations, and some early outs will cause worry among all ranks of the Army. Inevitably, this will extend into the civilian workforce, particularly with an estimated 20 percent pay cut caused by the recent start of 11 weeks of furlough.

While 99.9 percent of the individuals who are likely to be the hardest hit are loyal and dedicated American patriots, there nevertheless will be a small percentage whose financial hardships and other life stresses become so overwhelming that the resulting discontent and dissatisfaction will make them vulnerable to persuasion by foreign intelligence operatives, whose efforts to entrap these susceptible and exposed targets will require little effort at all.

The certainty of maybe not today

As accurate and apropos as the adage, "if you play with fire you will get burned," is, it is vital to understand that if you commit espionage, you will be caught.

The Army's military intelligence and counterintelligence organizations are designed to protect soldiers and employees from espionage threats and FISS espionage overtures. These entities and their work remains key to protecting the technological advances that give American soldiers the edge on the battlefield. Army counterintelligence have partnered with the FBI and have taken down important foreign recruitment operations. While trifecta targets may, in turn, be a target rich environment for FISS recruitment, one should assume that Newton's third law of motion applies to counterintelligence: for every action, there is an equal and opposite reaction.

To be specific, Army counterintelligence units have, and continue, to partner with the FBI on very important espionage investigations. Disgraced former US Army National Security Agency SIGINT analystDavid Sheldon Boone's 24 year and four month sentence for espionage on behalf of the former Soviet Union is proof positive that treason will be dealt with. Boone was arrested following a successful sting operation by the FBI in 1999 that was supported in large part by Army counterintelligence. According to press reports at the time, Boone decided to become a Soviet spy in order to alleviate "severe financial and personal difficulties" -- a familiar refrain sung by many other American traitors in financial trouble.

Remaining true to the core values

It is not by accident that loyalty is the first word cited in the Seven Core Army Values. It is also isn't accidental that the US Army is composed of both solders and civilians who know the importance of the mission at hand, and therefore go well above and beyond what is expected of them in their service to their country.

Nevertheless, because of current operating environments, tempos and the resulting pressures, there should be no doubt that there's a well-trained cadre of highly proficient foreign intelligence professionals out there who are operating in overdrive. Like barbarians breaching the gate, or a pack of hungry wolves surrounding a campfire, we have no alternative other than to remain more vigilant than we've ever been, especially given that our enemies today have far better knowledge and understanding of the stresses that are on

America's Army workforce. This is why supporting your battle buddies, knowing your left and right flanks and having your six covered will get us through this time of seemingly unprecedented tribulations with our core security values intact.

It's easy to imagine especially hostile foreign governments and their intelligence services plotting and rejoicing as they undoubtedly regard our furloughs and sequestration as a euphemism for discount espionage.

And a "discount espionage" opportunity almost assuredly is apparent in the minds of our avowed adversaries, as they understand that it's now far cheaper to buy not just one, but perhaps many, Benedict Arnolds today than it was during, say, the Cold War era of President Ronald Reagan. The return on a foreign intelligence service's investment has been made inherently worth the risk because of the cut-rate prices they can get away with paying today to comprise disgruntled, financially overextended and security cleared individuals. Like it or not, these individuals are perceived as virtually undemanding targets for espionage recruitment operations.

It is for this reason we must aggressively boost our awareness, redouble our vigilance and steadfastly support our fellow co-workers. The Army has a series of vitally important programs in place to take care of our people, yet they're often underutilized. And they're not new programs -- many were launched more than half-a-century ago. But over time, they've become overlooked, underappreciated and underutilized. For those in uniform who may be experiencing a financial crisis, the Army Community Services, Employee Assistance Programs and organizational Chaplains are there to counsel and provide spiritual guidance. Financial counseling and assistance is also available.

Your Army, as well as those who lead it -- are ready, willing and able to do their part. But it's also the duty and responsibility for all government employees, uniformed or civilian, to be vigilant and help your fellow soldier and office worker. It is one Army, and one team -- and we are dependent on that more today than ever before.

Remember, inaction begets targeting. Targeting invites compromise, and compromise precipitates contrition. But forgiveness for treason remains unattainable.

About the Authors

James R. Lint served in the United States military for over 20 years, in both the US Marine Corps (7 years) and US Army (14 years). He spent three years in Marine Infantry, four years as a Marine Counterintelligence specialist, and nearly 15 years as an Army Counterintelligence Special Agent. Lint has expertise in counterintelligence, cyber intelligence, security, information assurance, terrorism studies, counter-terrorism, human intelligence collection and low-intensity asymmetric warfare.

Previously, Lint served as Deputy Director for Safeguards & Security, Office of Science, at the Department of Energy. And prior to that, he served at the Department of Homeland Security Office of Intelligence and Analysis, where he was initially the lead cyber intelligence analyst and later the Chief of the Collection Analysis Team.

His military assignments include Korea, Germany and Cuba in addition to numerous CONUS locations. He currently serves as an Adjunct Professor at American Military University.

Lint is also the Chairman/CEO of the Lint Center for National Security Studies, a non-profit 501c3 that provides merit-based scholarships to students pursuing degrees in international relations, national security, and cultural awareness.

Timothy W. Coleman is a writer and security analyst who has co-founded two technology startup firms. He has a Masters of Public and International Affairs in Security and Intelligence Studies, and a Masters of Business Administration in Finance.

Coleman also serves as the Lint Center for National Security Studies chief operations officer.

The views expressed in this article are those of the individual authors and do not necessarily reflect official policy or the position of the Department of the Army, the Department of Defense or any other department or agency within the US Government.

Professional Certifications

Professional certification in OPSEC is a lot easier than you think. One of the key benefits of the OPSEC Professionals Society is the opportunity to earn the professional standing as either an OPSEC Certified Professional (OCP) or an OPSEC Associate Professional (OAP). The authority to use the OCP or the OAP proficiency designator after your name provides colleagues and employers with information about your level of proficiency in our profession. See the Certifications page on the OPS website.

Our Counterterrorism Tools Are Working

We should not throw out some of our best national security tools for the sake of satiating a political bloodbath.

by J. M. Peterson, Consultant/Instructor
Special Projects Director, Counterterrorism & Security Education and Research Foundation

Dear associates,

I hope that you will find the following of interest. Its in response to what is talked about in the linked article.

(Comment: Quote me if you like on below statement /Op-Ed as many of us have had enough of this whole leaks tragedy and its destructive aftermath- bottom line - we need to keep these programs in place.)

We just need to ensure better accountability, insulation of the iC and Ct community from political misuse, and abuse from within -perhaps look a little harder at more ethical behavior by those that we entrust at our expense. See below.

.....

For reference:
http://www.newsmax.com/Newsfront/chambliss-terror-plot-nsa/2013/08/04/id/518593?s=al&promo_code=1467B-1

Here it is.

This is not a mere opinion - it is my observation based upon first hand experience (not from sources on facebook, Wikipedia, google, political entities and agitators, nor the mainstream aka lamestream media) - from what I have seen myself:

Believe it or not, the vast majority of federal personnel in the intelligence community (includes NSA, CIA, DIA, etc.), homeland security (DHS), Department of Defense (DOD), and federal law enforcement (DOJ, FBI, etc.) involved in counterterrorism are patriotic, hardworking, highly skilled, and very dedicated citizens who would never do anything to hurt this country nor violate our rights. There are countless unsung heroes there.

Most all of their successes you will never hear about, as that would compromise those vital capabilities and hard-earned equities. Most of the intelligence gathering tools that you have been hearing about are ones put into place as a result of our intelligence failure that led to 9/11. The bottom line is that we need them to to preserve our way of life. We need them to survive. If you know anything about the most likely or most dangerous enemies courses of action (COAs), then you know that the terrorists have an entire menu to choose from and they continue to perfect their tactics, techniques, and procedures (TTPs) used to ply their nefarious trade.

Yes, we can do this while protecting the individual civil liberties of our citizens. Most all of our analysts, specialists, collectors, and law enforcement personnel could care less about what is in someone's personal email, text messages, or phone calls. Anyone that has been involved in indications & warnings (I&W), CT, threat finance, network targeting, or CT on the ground are simply overwhelmed.

Where Snowden and Manning found so much excess time to make all of their earthshattering discoveries, most of us would never know. The rest of us were too busy trying to keep an elusive, nefarious enemy, militant extremists and international terrorists, from endangering our people. (Also -notice how there are not hoards of intelligence personnel coming forward with similar claims as they did? If there were any validity or veracity to Snowden's claims, there would be plenty of bonafide whistleblowers.)

Unfortunately, many in the public are suffering from a combination of the common 'short memory syndrome' (that often leads to us collectively repeating our mistakes), and the influence of a wildy contentious, media driven political maelstrom emanating out of Washington D.C.

So, don't believe all of the claims and hype started by 2 malcontent, poor performers named Snowden and Manning, who in unpatriotic, criminal, and treasonous fashion leaked many of our nation's secrets and caused serious danger to our national security.

We should not resort to whimsical foolishness and snap judgments compelling us all to go summarily dismantling entire programs and vital organs of our national defense due to the word of two criminals (and media agitators, most all who just don't have their own facts straight and are doing more harm than good).

A troublesome aspect of this: Some very uninformed citizens are trying to label these two as 'heroes.' Some of us have had the honor of working in the company of real heroes and having met many more bonafide ones.

Snowden and Manning are not heroes in any sense of the word and its an insult to all of those who have actually taken great risks for our country to refer to those two as anything more than a defendant or criminal and

anything less than a traitor. (Note: Manning provided classified material to a website owned by a foreign national. Snowden's only course of action in exposing what he claims are misdeeds was to provide classified information to a foreign newspaper and then seek asylum in a country that has spied on our country more than any in the world for the past 90 or so years. They both have been subject to numerous classes and indoctrination or 'indoc' briefings as a holders of TS/SCI clearances, so they knew exactly what were doing)

Some heroes. Both of them hid behind computers while the rest of us were out there taking real risks and fighting the fight. Let me put it more simply - neither has ever so much as even seen a terrorist nor been shot at. But, they put the rest of us at risk.

Our real heroes don't go violating their oaths and duties just to get 15 minutes of fame.

The only ones helped by these leaks are our enemies. This entire set of national security leaks , aka unlawful disclosures of classified information, has been very overblown in the public domain.

Much of this was due to the aftermath and understandable psyche of disgust and loss of public trust in this current administration due to the very real IRS, DOJ, EPA, and other scandals. But, those have nothing at all to do with the grandiose and still unfounded claims of fugitive from justice Snowden.

We should not throw out some of our best national security tools for the sake of satiating a political bloodbath or because of uninformed bloggers and rampant incorrect facebook posts. If we do so, we are asking for another 9/11 (or at least samples to keep reminding us that Al Qaeda is still out to get us).

We have built an effective national security and counterterrorism apparatus in the past 11 years and 11 months. Its been very expensive and done with much toil and behind the scenes effort. As part of the intelligence cycle and the counterterrorism effort, lives are risked every day.

Let's not throw it all away because of questionable and largely unfounded claims by leakers and subsequent sensationalized 'journalism' that has come from both sides politically.

The bottom line is that our counterterrorism tools are working. And they are working for us, not against us, as some will try to make you believe.

Some us have seen firsthand what our enemies, the terrorists, can do and its pretty ugly. And, they are showing no signs of giving up.

Let's keep these hard-earned capabilities in place and keep fighting the fight. If the public had all of the facts, that is exactly what they would be asking for.

Upcoming Event

Tuesday, 5 November: EMSolutions, an OPS Bronze Corporate Sponsor, will host "OPSEC in the Federal Government: A Government-Industry Challenge." The one day event will be held at 1401 S. Clark Street, Suite 500 in the Droz Theater. The unclassified program will include a key note addresses by senior government and industry officials; featured speaker Greg Howe, author of "*A Perfect Storm The Operations Security Support Division – From SAVE to SAP*"; and a superb mix of implementation, program, and academic presentations. There is no charge or fee for attendance. Attendance is limited to those registered. To save a seat and register, send name, organization, position/title and phone number(s) to OPSEC@EMsolve.com<mailto:OPSEC@EMsolve.com>

8:00-8:30 AM: Registration and networking
8:30 AM: Theater doors close, program begins
4:00 PM: Program concludes

(Working lunch: $10 collected at registration or cafeteria is available within a short walk)

4:15 PM: No host networking social at the Potomac Grill starting at 4:15 PM (Potomac Grill is in the Crowne Plaza across the street from the Droz Theater)

Detailed program information and content will appear in newsletters and press releases starting on 12 September 2013.

Suggested Reading

My name is John Davis. I 've presented several times at the National Opsec Conference. In fact, I taught the threat portion of the DA OPSEC course for ten years. After almost a year in seclusion after retirement from the government, I've finally published my book, *Rainy Street Stories*. It recounts events from my life, and people I met, during the Cold War. It is a series of reflections which thus far has been endorsed by a Pulitzer Prize winner, and gotten several good reviews, one of which I include below. I hope you like it, and recommend it to others.

Here is the link to Rainy Street Stories on Amazon. http://www.amazon.com/RAINY-STREET-STORIES-John-Davis/dp/1936800101

Here is a review published in the SoHo Journal in Manhattan: http://sohojournal.com/content/art-intelligence-rainy-street-stories

The OPSEC Professionals Society — Committees

We have several active committees and we encourage you to join one.

Membership & Communications: Duties include receive and process applications for membership, to decide on eligibility of prospective members subject to the review and judgment of the Board of Directors and to promote the increase of Society membership. If you are interested in this committee, please contact Communications@OPSECsociety.org.

Revenue: Duties include to verify all Society assets and liabilities, examine all records of the Treasurer to insure that standard, basic accounting procedures are being used, insure that bills are being paid promptly and fully identify the material or service provided, at or near year-end, review expenditures in relationship to the Annual Budget and make recommendations for the next year's budget plan and examine such other records as the Committee Chairman might deem necessary. If you are interested in this committee, please contact Communications@OPSECsociety.org.

Education: Duties include develop and oversee the production and execution of programs and seminars of interest to the membership, as well as educational programs for the benefit of government agencies and private sector corporations. If you are interested in this committee, please contact Communications@OPSECsociety.org.

Professional Standards: Are you interested in promoting OPSEC professionalization? Do you have an extra four to six hours a month? Are you or do you intend to be certified as an OPSEC professional? The OPS Standards Committee provides an exceptional opportunity to promote the practice of OPSEC. The committee establishes and maintains defined criteria necessary for professionalization. All applicants are subjected to a review process to ensure consistency in the professionalization process. Participation in this process is an opportunity to create your legacy and help create a heritage for generations of future OPSEC practitioners. If you are interested in this committee, please contact Standards@OPSECsociety.org.

Membership Renewals

Attention Members! You can now download the new membership renewal form online and pay by credit card, and/or; you can now pay your renewal dues via PayPal!! Go to the Membership Renewal page: http://www.opsecsociety.org/memrenewal.htm.

Corporate Membership

Corporation memberships are available for as little as $500 which allows up to five individual corporate memberships. Membership also includes advertising space in this newsletter and the website. More information is available in the corporate memberships fee schedule,

Important Links

Interagency OPSEC Support Staff
http://www.iad.gov/ioss/

Information Assurance Support
http://iase.disa.mil/eta/

National Counterintelligence Executive
http://www.ncix.gov/

US Patent Trademark Office
http://www.uspto.gov/

ABOUT OPS

Our membership is comprised of United States government, military, corporate and private practice professionals and those of our nations allies who specialize in the field of OPSEC, Counterintelligence, and other related disciplines. The society is governed in accordance with OPS By Laws by a Board of Directors elected from among the membership, and members staff committees and various working groups in furtherance of the OPS mission. National Officers are elected from among members of the Board.

CODE OF PROFESSIONAL ETHICS

and conduct for members of the
OPERATIONS SECURITY PROFESSIONAL SOCIETY

OPS Members Shall:

- *put loyalty to the highest moral principles and to country above other loyalties.*
- *continually strive to increase respect, confidence, trust, and recognition of the profession in both the public and private sectors.*
- *demonstrate a personal commitment to professionalism and diligence in the performance of his/her duties.*
- *not engage in any illegal or unethical conduct, or any activity which would constitute a conflict of interest.*
- *exhibit the highest level of integrity in the performance of all professional assignments and exhibit the highest levels of professional competence.*
- *not reveal or use information received in confidence during a professional assignment without proper authorization.*
- *report all information obtained during the course of an assignment accurately and completely.*
- *continually strive to increase the professional competence and effectiveness of those serving under his/her direction.*
- *refrain from gratuitously making adverse comments about the work, knowledge, fitness, or other qualifying aspect of another OPS member.*
- *promote and encourage full compliance with these standards within the entire profession.*

OPSEC PROFESSIONALS SOCIETY
PO Box 150515,
Alexandria, VA 22315-0515

Communications Committee- Newsletter
Victor "Top" Watson
Dale Carter
Carla Gregor
Scott Mirchin

To learn more about advertising and sponsorship opportunities or to make a donation: contact president@opsecsociety.org,

To submit information about an upcoming event; or you are interested in submitting an article to the OPSEC newsletter – send your proposed article to: communications@OPSECsociety.org

EMAIL: Communications@OPSECsociety.org
To ensure delivery to your inbox (not bulk or junk folders), please add Communications@OPSECsociety.org to your address book

TO SUBSCRIBE: If you were sent this by a colleague and wish to subscribe the cost to non-members is $10 per year payable by check or credit card. Please send a subscription request for the OPSEC Professionals Society's E-newsletter to: Communications@OPSECsociety.org

TO UNSUBSCRIBE: This news service comes to you from the news team at the OPSEC Professionals Society. If you do not wish to receive it in the future, please reply to this e-mail with the subject line "Un-subscribe

Points of Contact

OPSEC Professional Society National Executive Board:

President - president@OPSECSOCIETY.ORG

Vice President - vicepresident@OPSECSOCIETY.ORG

Secretary - secretary@OPSECSOCIETY.ORG

Program and General Information

Inquiries regarding professional certifications (OAP, OCP) contact our Professional Standards Committee at: standards@OPSECSOCIETY.ORG

General questions and membership inquiries should be directed to: communications@OPSECSOCIETY.ORG