

20 February 2009

Volume 1, Issue 5



Chairman's Corner

InfraGard National Members Alliance, a 501(c)3 not-for-profit organization

In This Issue:

- New Initiative, pg 2
- INMA Spotlights, pg 3-4
- Chapter Spotlight, pg 5
- Credentialing, pg 6
- Research and Legislative Corner, pg 7
- Announcements, pg 8
- Events, pg 9

Please report any membership information changes (i.e., email address, mailing address, etc.) to infragardhelpdesk@infragard.org.

Questions or Comments

Dr. Kathleen Kiernan
Chairman@infragardmembers.org

Sheri Donahue
ManagingDirector@infragardmembers.org

(703) 772-2294

www.infragardmembers.org



Dr. Kathleen Kiernan
INMA Chairman of the Board
Jacksonville IMA

Hello to all. As always, thank you for your dedication to this organization. I hope that is a compliment you never tire of receiving as I will never tire of acknowledging that the true measure of success we enjoy is the result of the members who volunteer their expertise and their commitment to public service. I had the opportunity to participate in a GAO review on cyber security this past month and spoke at length about our volunteer membership and the significant contributions they bring to both homeland and national security. I was delighted to have the opportunity to participate, but more so because in the following days I received email from fellow panel members who have decided to join InfraGard. Look for an update on the new leadership at the Department of Homeland Security in the next issue where the emergent theme being reinforced is the partnering of the public and private sector. As well, we continue to see evidence of the Administration's commitment to rebuilding and securing the nation's critical infrastructure.

In this issue you will find a number of updates on issues and events which directly impact our organization. At the national level we are in the midst of working through a budget for the next year and trying to maintain a high level of service with a current budget that is insufficient. Thank you to all of the Chapter Presidents who have stepped up to work through these issues under the great leadership of Ron Dick, Dyann Bradbury, and Freeman Mendell. Our Managing Director, a key to our historical success, is currently volunteering on a part-time basis but true to her dedication. Sheri Donahue continues to shoulder a majority of our responsibilities. We are not immune from the economic crisis which is affecting our nation - and we will survive and continue to thrive even with the current restrictions. There has been significant progress made with the SANS initiative and as well with our partnership with CISA. Each will broaden the outreach and educational opportunities for our membership and each carries the strong potential to raise revenue. I had the pleasure of speaking at a joint InfraGard/ISSA event in Chicago and found a tremendous synergy between our organizations. My thanks to John Jackson and Wayne Johnson, the co-hosts who packed the house and inspired

increased collaboration. In addition, we received excellent support from the Chicago office of the FBI and had an opportunity to publicly thank the outgoing coordinator, SA Brent Dempsey, and to welcome in the new coordinator, SA Robert Kowalski.



This past month, former INMA Board member Rich Garcia and I had the opportunity to make a presentation to the National Sheriffs Association on the issue of credentialing, which was extremely well received. That week we also met with the Department of Homeland Security and are working to have InfraGard members included in two upcoming national exercises. A special thanks to Dennis Kelly (Southeast Louisiana IMA President) and to Pegasus. I had the opportunity to meet with the Senior Advisor to the Director of National Intelligence (DNI) on public outreach and will participate in a DNI-sponsored public forum later this month on "partnering for effect" with the private sector with the leaders of many other organizations.

In the near future we will be reaching out with an update on the upcoming Congress to discuss the potential of hosting a secure VTC with the membership, coordinated at the FBI HQ level with the Director as a keynote speaker. We recognize that as substantive as this kind of interaction is, it does not completely substitute for the in-person interaction of our volunteer leaders in conjunction with GFIRST as we have done in the past, however for this year it may be a fiscal reality. Before we make that decision, we will reach out and survey the presidents. I have asked all of our board members and officers to reach out to our various chapters on an ongoing basis to ensure we always have ground truth and this has been a great experience. I learn so much with each personal outreach about the members, leadership style, and as you will see in the profile of the Los Angeles Chapter, great initiatives. We will continue to profile a different chapter each month and will also be featuring different volunteer leaders in upcoming issues. Again thank you for your support and for your confidence. Kathleen

InfraGardAwareness! Initiative with The Center for Information Security Awareness (CISA)



Dyann Bradbury
INMA Board of Directors
Nebraska IMA

On December 15, 2008 the INMA Board of Directors approved partnering with The Center for Information Security Awareness (www.thecisa.com) to provide free training focused on using the workplace as the foundation for better security education and training.

A growing number of studies have identified employees and other insiders as the cause of the majority of data and security breaches and better security awareness and training is central to reducing these incidents.

The web-based course, created by the CISA, is professionally narrated throughout and consists of 14 separate lessons covering key information security issues that can impact the workplace, including:

- The cyber threats to the workplace and the nation
- The value of awareness
- The role of employees
- Understanding the threats
- Understanding how employee behavior is exploited
- The importance of regulatory compliance
- Better workspace security
- Passwords
- Understanding social engineering
- Better email practices
- Safer surfing practices
- Protecting sensitive data
- Understanding and avoiding identity theft
- Appropriate use of workplace resources
- Laptop security
- Security outside the workplace
- Compliance and regulatory issues such as PCI, Sarbanes-Oxley, and FISMA

This interactive and engaging training targets issues central to Critical Infrastructure Protection (CIP) by addressing topics such as: why security matters; the potential impact of cybercrime and identity theft on the company, its customers and on employees; the important role employees play in information security; and, the importance of following internal security policies and rules to avoid data security breaches.

The course also addresses security best practices, the goals of security policies in the workplace, and how employees can help their workplace meet these goals.

As mentioned, anyone can take the free course. For a nominal fee of \$25, those who wish may take an online test and, if they pass, will immediately be issued an InfraGard Certificate in Information Security Awareness. The examination consists of 100 randomly-generated questions relating directly to the course materials and an individual may take the exam as many times as necessary to achieve a passing score.

InfraGard members will have access to a discount code, allowing them to get certified for only \$20.

The InfraGardAwareness! initiative dovetails on multiple levels with InfraGard's overall mission by:

- Providing meaningful, dynamic, interesting and critically important information security awareness to Americans at no cost to them or to InfraGard
- Helping American businesses of all sizes to improve their security without incurring additional costs
- Supporting InfraGard's focus on Critical Infrastructure Protection
- Increasing InfraGard's visibility, reach and membership
- Enhancing InfraGard's reputation and viability
- Providing a passive income stream to support and sustain InfraGard's important missions

The costs associated with creation, narration, production, programming, hosting and updating this initiative are being borne by the CISA. Not only are all costs incurred by the CISA, but they are donating a percentage of the revenues generated from the Certificate in Information Security Awareness.

Please look for a formal press release on this important initiative near the end of February. Also, please do all that you can to bring this high-quality, free training opportunity to the attention of your members, business partners and the community. Every time someone gets certified, InfraGard becomes financially stronger. Your support is sincerely appreciated.

More information about this initiative and the free course may be found at www.InfraGardAwareness.com. More information about The Center for Information Security Awareness may be found at www.TheCISA.com.

New FBI Powers: A Necessary Step for Counterterrorism



Michael Rolince
INMA Board of Directors
Nation's Capital IMA

On October 3, the Department of Justice published the revised Attorney General Guidelines (AGG), which govern all Federal Bureau of Investigation (FBI) activities, including those involving international terrorism. The AGG came into effect on December 1, 2008, and consolidated procedures controlling the FBI's various investigative programs. Although members of Congress, civil rights groups, and the media have criticized the AGG, the revision is a necessary and important step for the FBI's counterterrorism investigations as well as all of the Bureau's investigative programs. Justice Department and FBI officials, however, will have to exert strong leadership to ensure the appropriate and effective implementation of the guidelines.

One potential advantage of the new guidelines is the ability of the FBI to resolve threats and conduct investigations and assessments which, heretofore, required significantly stronger predication. Engaging local FBI Coordinators for the purpose of explaining the new guidelines and reviewing their potential impact is a prudent measure.

Background

Until 1976, no formal Justice Department guidelines governed the FBI's investigative activities. Since the Congressional Church and Pike Commissions, which exposed troubling activities of the FBI and the intelligence community, U.S. intelligence and law enforcement agencies have been subject to far greater regulation and oversight. Former Attorney General Edward Levi put in place several notable guidelines, separating the FBI's criminal investigations from those related to national security and intelligence. (The criminal guidelines were released, but the intelligence guidelines remained classified.)

The FBI's two distinct responsibilities -- serving as both the country's domestic intelligence agency and its chief federal law enforcement agency -- increasingly hampered the Bureau's counterterrorism efforts. In the 1990s, the now famous "wall" between intelligence and criminal activities made information sharing increasingly difficult, even on related investigations. The FBI also had different tools available in the criminal and intelligence arenas. For example, the FBI could use administrative subpoenas to acquire a small-time drug dealer's phone records almost immediately, yet it did not have this same authority when dealing with U.S. associates of the September 11 hijackers.

While the situation changed a number of times over the years, the FBI has, until now, continued to operate its criminal and intelligence investigations under distinct guidelines. The new AGG are an attempt to address this issue by consolidating all the procedures into one clear set of guidelines.

Impact

The confusion among FBI agents, officers, prosecutors, and managers engendered by the September 11 attacks is well documented. On the day of the attacks, the Bureau had approximately 500 agents assigned to international terrorism investigations in 56 main offices and 400 smaller offices throughout the United States, and in some 40 U.S. embassies around the world. Two days later, the number of agents exceeded 7,000. Agents who were investigating violent criminals, corrupt politicians, drug dealers, and organized crime families from New York to LA found themselves chasing al-Qaeda from Kabul to Kansas. And they were doing so with little or no training and guidance regarding the rules of the road.

Investigators and supervisors will welcome the new AGG for reasons of simplicity, clarity, and efficiency, particularly in the realm of counterterrorism. For the first time in the FBI's hundred-year history, one set of guidelines will govern the conduct of all criminal, intelligence, counterintelligence, and counterterrorism investigations.

Having one set of clear guidelines will streamline the responsibilities of those charged with ensuring strict adherence to the law. For instance, if the current financial crisis requires the redeployment of agents from counterterrorism to the white-collar crime program, the new guidelines will be a welcome. With a working knowledge of exactly what agents can and cannot do during a lawful investigation, the FBI will meet with success.

Widespread Criticism, Need for Oversight

The Justice Department's announcement of the new guidelines has, not surprisingly, opened it up to widespread criticism from the media, Congress, and civil liberties groups. In the view of one civil liberties advocate, the new guidelines give the FBI too much latitude "to open investigations of innocent Americans based on no meaningful suspicion of wrongdoing."

Perhaps the most noticeable change in the AGG is the easing of the strict standards governing the initiation and continuation of active investigations to allow, in some cases, the use of surveys, or "assessments," to ascertain the potential threats warranting further scrutiny. According to critics, this provision opens up the potential for agents, especially inexperienced ones, to pursue questionable investigations for unjustifiable periods of time. Specifically, there is concern that this may encourage the violation of U.S. civil rights through the harassment of innocent persons, particularly in Muslim and Arab communities.

Although these concerns are not entirely without foundation, FBI supervisors and agents are willing and able to implement the new guidelines with due respect for the rights of the American people. FBI and Justice Department leaders must ensure that these new tools are used appropriately and effectively. The FBI should continue aggressive efforts to ensure its entire staff -- from senior executives to analysts -- fully understands the new AGG. Ensuring clarity, consistency, uniformity, and repetition during training will help guarantee that the streamlined AGG are used to maximum effect, while protecting the rights and liberties of the citizens every agent is sworn to protect.

Continued on page 4

Continued from page 3

The new guidelines may place FBI agents in greater contact with Arab Americans and other ethnic minority communities; this would, indeed, be a positive outcome. The FBI should seize the opportunity to redouble its efforts to eliminate ad hoc management of crucial community relationships and adopt an approach that is consistent, productive, and comprehensible by all. Since the September 11 attacks, the FBI has worked diligently to establish contact with the Arab American community and develop the means and methodologies to foster collaboration against a common threat. Only through constant, meaningful and reasoned dialogue with these and other groups will the FBI gain a realistic appreciation of their views. Hopefully, the communities that often feel targeted will come to know the faces, intent, and culture of those who solicit their help.

Conclusion

The FBI has been entrusted with unparalleled authority to "chase the threat" without the constraints that governed the agency for many years. With increased authority, however, comes increased responsibility: proper training, retraining, coaching, supervising, and managing within the guidelines' framework have never been more important. Although this task will not be easy, it is not impossible. And since the FBI cannot succeed in fulfilling its mandate without the unwavering support and confidence of the American people and groups such as ours, the FBI has to get it right. Individuals should acquire a basic understanding of how this enhanced capability may prove useful in conducting investigations around threats to our infrastructure, our personnel and our property. Continued cooperation, collaboration and vigilance will remain key to this effort.

A New Administration



Michael Hershman
INMA Board of Directors
Nation's Capital IMA



InfraGard Members eagerly await the new Administration's plans on homeland security and in particular critical infrastructure protection.

To date the new President has appointed a strong team of national security and law enforcement experts to manage the defense of our Country. This team will need to focus a great deal of effort on the changing economic environment - how this will affect the nature of threats to our critical infrastructure, and how with dwindling resources we are to confront those threats.

There are some early indications of the direction the new President will take. President Obama has proposed a sweeping economic stimulus plan which includes billions of dollars for rebuilding the country's infrastructure. I was pleased to see among the proposals money to enhance the security at 90 major ports in the United States. This demonstrates an early awareness that improvement in security infrastructure potentially holds the twin benefit of increasing our security profile while providing much needed jobs. But, let's not stop there. While funds are being allocated for bridges, tunnels, highways, water resources, and other projects, let us include in those a security component. We all know that

much more effective and less expensive to upgrade security in the planning stages of these projects rather than as an add-on.

Another positive indication of this President's thinking is in the way he speaks to transparency and accountability. We know that some prior funding decisions for homeland security were tainted by political influence and shortsighted choices. We need to bring greater daylight to the decision making process as it involves distribution of homeland security funds to the states. And, when those funds arrive we want to make sure that they are used for appropriate purposes. Our budget crises will require smarter choices and those choices require serious input from state and local government, the private sector and non-governmental organizations.

Increased transparency can also lead to better information sharing. This is a difficult topic which has been the subject of much discussion since the creation of the Department of Homeland Security. Despite countless intergovernmental meetings and years of dialogue with the private sector, there is still not a good method for the sharing of threat information and solutions. This Administration should move quickly to define standards and create an infrastructure to be used by the government and the private sector for data sharing.

LOS ANGELES

InfraGard Members Alliance

InfraGard Los Angeles has achieved critical milestones as a direct result of applying a business approach designed to support stabilization and growth and our ability to meet operational interests and responsibilities. This approach ended up as a guide to a 3-year plan which was developed around five critical elements; some elements of which are provided below:

1. Perform a critical review of the organization as it is today. This will help ensure you have clarity as to its current status. Look to see; (a) if you have controlled growth, (b) if the organization is simply stable, or (c) if the organization is stagnant?
2. Formalize its mission based on (a) its current assets and, (b) future requirements for stability and growth.
3. Develop both a project plan (*a detailed executive summary can suffice*) based on your re-stated objectives/mission and a timeframe for a related plan of implementation.
4. Develop/build your organization from the top down. This works well for this kind of organization. Without effective leadership, the management concepts of controlled growth and stability will be near impossible to implement and/or achieve. And, it is strong leadership and operational success that will be of critical interest to your stakeholders/partners.
5. Funding your organization is a must. Whether it comes exclusively from your members, or in part from local, state and/or federal agencies, it's all about understanding their needs and what you can deliver. Build a reputation for delivering what you have said you could. Think of funding not as an entitlement but rather as payment for services.

Below is additional information intended to provide definition and clarity to the five elements above.

Year #1: Stabilizing the Board of Directors and Officers by clearly identifying their role, their authority, and their fiduciary responsibilities. Also, introduce a progressive plan of training and education programs specifically and almost exclusively for Board and Officer level personnel. The goal was to have an educated and informed senior management group which, through its learned knowledge and hands-on experience, could effectively lead the organizations' membership in future programs and activities. Education and training was the key. From an academic viewpoint our efforts were centered on the premise basis that *education* provided knowledge whereas *training* developed skills.

Result: We have not lost a Board Member for three years and our Board members and Officers participate as highly effective leaders and active participants in key exercises.

Year #2: Identify Sector Coordinators for each of the key critical infrastructures as determined by InfraGard Los Angeles. In that process we looked to develop education and training programs

which would bring them together strategically with the Officers and Board of Directors. Also, we focused on arranging funding through Los Angeles County stakeholders (law enforcement). These stakeholders, due to the threat level of Los Angeles, share InfraGard's interest in counter-terrorism and have similar interests and mission to integrate resources and assets between law enforcement and the private sector... in a joint effort to mitigate both terrorist-based, and natural disaster-based, threats, risk and loss.

Result: InfraGard Los Angeles has executed a 5-year consulting agreement with Los Angeles to assist in developing and guiding such integrated efforts. This effort is based out of the Los Angeles Joint Regional Intelligence Center / Regional Terrorism Threat Assessment Center (LA-JRIC/RTTAC) within which InfraGard Los Angeles has an office. This allows InfraGard to collaborate closely with the multi-agency task force consisting of local, state, and federal law enforcement and intelligence agencies assigned to the JRIC. Almost all programs developed by InfraGard Los Angeles now include these departments and agencies and vice-versa.

Year 3: Develop an annual exercise which will allow large numbers of InfraGard Los Angeles members to participate. This is a daunting task considering that we represent the same 7 counties as the FBI Los Angeles Field Office. This office, and thus InfraGard, is concerned with a territory of some 40,000 square miles. The Central District of California is the most populous federal district in the country with more than 18 million residents. As such, it is critical that InfraGard Los Angeles be organized in its approach and not manage the organization based on perceived or non-related requirements but rather on our efforts to identify and meet the needs and interests of the community and our strategic partners.

Result: In May 2008, with leadership from the Center for Asymmetric Warfare (CAW), InfraGard and the JRIC, we hosted a war game based exercise entitled "Cyber Attack Detection Response Exercise 2008 (CADRE – 08)



In 2009, in conjunction with the CAW and the JRIC, we are developing a program centered on the threat to our schools from terrorist. We are planning for participation by 400-500 InfraGard members along with local and federal law enforcement.

Additionally, we hold an Orientation Program twice a year for new members. This has been wildly successful. FBI, US Secret Service, LAPD, LASD and Joint Regional Intelligence Center ("JRIC") personnel identify the resources/assets they have available for InfraGard Los Angeles members. Specifically, they delineate policies and procedures and protocols on how to communicate and interact with their agency as well as how you can assist them as subject matter specialists of critical infrastructure sectors. Designed for new members, long standing members are also invited if they have not yet participated in this valuable program.

Richard L. Jones
President/CEO
InfraGard Los Angeles

Non-Government Access into a Crisis Area - A Follow-up to the Credentialing of the Private Sector



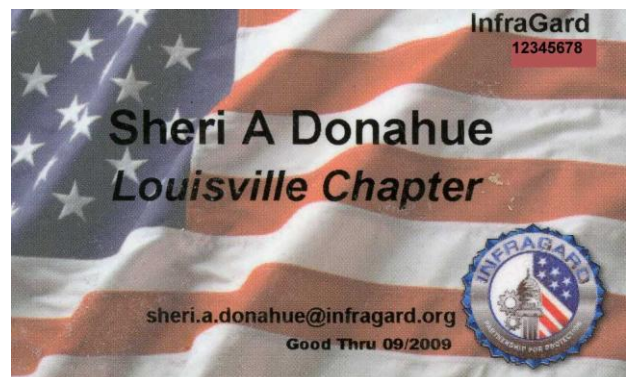
Richard T. Garcia
Former INMA Board of Directors
Houston IMA

In the November newsletter, we discussed the acceptance of the InfraGard National ID Card as an approved credential for entry into an area blocked by government officials during the recent hurricanes in Louisiana by the Louisiana State Police. Since then, the InfraGard National Members Alliance (INMA) has been engaged with the National Sheriffs Association's Pegasus Program. This program embraces emergency responder credentialing and collaborative technologies, which support voluntary credentialing of public and private sector credentialing and identity authentication for incident management, crisis area reentry and related purposes. In addition, InfraGard has had some preliminary meetings with DHS and representatives of the Energy Sector through the Energy Security Council (ESC). The article we published in the November newsletter has caught the eye of many who believe there is a solution to this process.

In December, the INMA met with representatives from the New Orleans FBI, NSA, Mississippi River Maritime Association and ESC. A consensus was reached from the groups represented and the following action plan was prepared. The INMA will participate in a pilot project with DHS entitled "Winter Chill" in March and another exercise in May of this year. During this pilot, the INMA and Shell Oil (representing the energy sector in INMA) will test various types of FIPS 2001 standard cards and/or private sector company identification cards utilizing the Pegasus model. This will require thinking out of the box and the utilization of existing programs to see how we can "keep this simple". We all believe the end game is to "facilitate a trusted group into disaster areas" in the most proficient manner possible.

In January of this year, Dr. Kathleen Kiernan and I, representing the INMA, attended the NSA Winter Conference in Washington, DC. We met with the Pegasus group from NSA as well as DHS. A status report was provided to the Executive Board of NSA regarding the working relationship between the INMA and NSA-Pegasus as well as some highlights of the way forward. The INMA, through representatives of the energy sector, will host a meeting in Houston, TX in April to further discuss how to engineer and test the solution in the May DHS exercise. DHS will also attend the meeting in Houston and they have tentatively agreed to allow private sector ID cards to be utilized for this project. We will be discussing the mechanics of this process at this meeting.

So, to summarize, a concept and the use of the InfraGard National ID card by the Louisiana State Police during last year's hurricane season may have been the catalyst for this alliance between INMA, NSA and other agencies in order to come up with a working model credentialing the private sector. There is still a lot of work to be undertaken in the future, but we have a good alliance with those involved and all are determined to achieve our common goal.



Research Corner: Integrative Center for Homeland Security

For many of us the start of a new year is a cause to reexamine our goals and priorities in the workplace. As such, the New Year is a chance for us to move forward with a new resolve and renewed vigor to both tackle challenges and create new opportunities.

One of our goals for 2009 is the continuation of Research Corner as a source of information to help InfraGard members be more effective in their continuous efforts to secure the nation's 18 critical infrastructure segments.

This month in Research Corner we focus on key documents and testimonies concerning cyber security.

House Permanent Select Committee on Intelligence, Cyber Security Hearing

- Testimony of Paul B. Kurtz:
<http://homelandsecurity.tamu.edu/framework/criticalinfra/criticalinfr/cyber-computer/house-permanent-select-committee-on-intelligence-cyber-security-hearing-2013-paul-b-kurtz.html/>
- Testimony of John Nagengast:
<http://homelandsecurity.tamu.edu/framework/criticalinfra/criticalinfr/cyber-computer/house-permanent-select-committee-on-intelligence-cyber-security-hearing-2013-john-nagengast.html/>



Dr. David McIntyre
INMA Board of Directors
Houston IMA

Co-written by Laura Spencer,
Integrative Center for HLS

- Testimony of Amit Yoran:
<http://homelandsecurity.tamu.edu/framework/criticalinfra/criticalinfr/cyber-computer/house-permanent-select-committee-on-intelligence-cyber-security-hearing-2013-amit-yoran.html/>
- Securing Cyberspace for the 44th Presidency
- <http://homelandsecurity.tamu.edu/framework/criticalinfra/criticalinfr/cyber-computer/securing-cyberspace-for-the-44th-presidency.html/?searchterm=securing%20cyberspace>
- Information Technology Sector-Specific Plan of the National Infrastructure Plan
- <http://homelandsecurity.tamu.edu/framework/keyplans/interimnationalinfrastructureprotectionplanfolder/information-technology-sector-specific-plan.html/>

For more information on critical infrastructure and other homeland security issues, visit our research library, TEX, on our web site at <http://homelandsecurity.tamu.edu/framework>

Activity on the Hill



Jerry Dixon
INMA Vice President,
Government Relations
Nation's Capital IMA

Some government infrastructure protection highlights are:

1. The House has introduced a measure to insure more information from classified sources, specifically threat information, gets into the hands of state & local law enforcement. To paraphrase this requirement, any agency that produces classified threat information also will need to produce a de-classified threat document that will be actionable for first-responders. Congresswoman Jane Harman is the sponsor of this bill. Her goal is to tackle the over-classification of information.
2. The State of Wisconsin's Homeland Security Council has drafted a new Homeland Security Strategy for their state and it is open for public comment. The

- document can be found at <http://homelandsecurity.wi.gov/>
3. Congresswoman Yvette Clarke (D-NY) has been appointed Chairwoman and Congressman Daniel Lungren (R-CA) as ranking member for the Homeland Security Sub-committee on Emerging Threats, Cyber-security, and Science & Technology.
 4. On the Port Security front, many harbor workers will have to carry new "Transportation Workers Identification Credentials" (TWIC) and it will be enforced by the US Coast Guard. The rules for having a TWIC card go into effect this month.
 5. In California, the Governor merged the Office of Homeland Security with the Office of Emergency Management to simplify emergency response coordination within their state. The new combined office, California Emergency Management Agency, is responsible for incident management of natural disasters and terrorist attacks.
 6. Homeland Security Secretary Janet Napolitano has initiated a review of the department's infrastructure protection efforts and final reports are expected back to her office by the end of February.

Lastly, if you have news from your region on infrastructure protection efforts please pass them along so we can share those back out with all of the other chapters.

General Reminders and Announcements

NEW!

NIPP: The 2009 National Infrastructure Protection Plan (NIPP) is available at www.infragard.net/library/pdfs/nipp_2009.pdf. It may also be downloaded from www.dhs.gov/NIPP. Hard copies of the document will not be available for several weeks but may be requested from NIPP@dhs.gov.

This document is posted on the InfraGard Public website, therefore no login is required. Please contact InfraGard Tech Support at (877) 861-6298 or infragardhelpdesk@infragard.org for assistance.

Secure Email: If you are an InfraGard member and have not received this newsletter directly from the InfraGard Secured listserv, please contact the InfraGard helpdesk to update your email address (infragardhelpdesk@infragard.org).

INMA Minutes: The INMA Board and Officers held its monthly meeting via conference call on 11 February. The minutes from this meeting will be made available following Board approval. These and all Board meetings are available in the Library on the InfraGard portal on CyberCop. Information on how to register for a CyberCop account is available at www.infragardmembers.org under Member Resources.

Presidents Handbook: Also available on CyberCop is the Presidents Handbook. All IMA Presidents are encouraged to have a hard copy of the Presidents Handbook in a binder in which they also keep all IMA business documentation (i.e., incorporation documents, 501(c)3 documents, copies of agreements with the INMA (Sub-License Agreement and Voting Member Agreement), Board and member meeting minutes, bank account

information, etc.) Once the office of the IMA president transitions to the next president, the outgoing should provide the incoming with the "IMA Binder".

Presidents' Listserv: Each IMA President is allowed to be listed on the Presidents Listserv administered by the INMA. Additionally, each IMA president may include up to two other members of their local leadership (i.e., board members, officers) to be listed on the Presidents' Listserv in order to ensure ongoing communications. Please contact ManagingDirector@infragardmembers.org for further information on the Presidents' Listserv.

LSU Listservs: LSU provides two listservs per chapter. One is for the local board and the other one is for the local membership. Please contact infragardhelpdesk@infragard.org for further information on these listservs.

Please report any membership information changes (i.e., email address, mailing address, etc.) to the InfraGard helpdesk at either (877) 861-6298 or infragardhelpdesk@infragard.org.

Please report changes in the name of the President or the President's contact information to the INMA Secretary at secretary@infragardmembers.org.

Secure Site: The Public Private Alliance Unit (PPAU) at FBI Headquarters, the unit responsible for the overall FBI management of InfraGard, posts notices, monthly and semi-annual reports on the secure website at www.infragard.net. All InfraGard members are asked to log-in to this portal at least once every 90 days in order to renew their passwords. If you have been locked out or are having trouble, you may contact the helpdesk at (877) 861-6298 or infragardhelpdesk@infragard.org.

Contact the helpdesk at infragardhelpdesk@infragard.org to update your email address if you are an InfraGard member and did not receive this newsletter directly from the InfraGard listserv.



PHONE:
(703) 772-2294

E-MAIL:
Chairman@infragardmembers.org

Visit us at:
www.infragardmembers.org

Upcoming Conferences

CSI SX (Security Exchange)

17-21 May 2009
Las Vegas, NV

<https://www.cmpevents.com/CSISX9/a.asp?option=B>

INMA Vice President for Government Relations Jerry Dixon scheduled to speak

RSA Security Conference

20-24 April 2009
San Francisco, CA

www.rsaconference.com

INMA Vice President for Government Relations Jerry Dixon scheduled to speak



About InfraGard and the InfraGard National Members Alliance...

The InfraGard Program began in 1996 as a collaborative effort between private sector cyber professionals and the FBI field office in Cleveland, Ohio. The FBI later expanded the program to every field office in the country. In 2003 the private sector members of InfraGard formed the "InfraGard National Members Alliance" (INMA). The INMA is a non-profit Delaware LLC with 501(c)3 status. The INMA LLC is comprised of 86 separate 501(c)3 InfraGard Members Alliances (IMAs) that represent over 29,000 FBI-vetted, InfraGard Subject Matter Experts. The INMA has a dual-focus value proposition. It provides its members with unmatched opportunities to promote the physical and cyber security of their organizations through access to a trusted, national network of Subject Matter Experts from the public and private sectors. And, it provides government stakeholders, across the local, state, and Federal levels, with unmatched access to the expertise and experience of critical infrastructure owners and operators. For more information about InfraGard, please visit www.infragard.net. For more information about the INMA, please visit www.infragardmembers.org.