Sacramento InfraGard Members Alliance

Sacramento IMA Quarterly

Second Quarter

The *IMA Quarterly*, coordinated, edited and distributed by the IMA Operating Committee, will provide information sharing environment and chapter event updates to our membership on relevant Homeland Security and Public Safety issues.

- This piece is Unclassified and can be shared with other InfraGard members and appropriate industry professionals.
- Articles from this newsletter are the opinion of the author and do not represent the official opinion of InfraGard or the FBI.
- Output will be primarily electronic, distributed in a PDF format.

INSIDE THIS ISSUE

SPECIAL POINTS OF INTEREST

- New Website
- Active Shooter
- Cyber Hygiene

Presidents Message

Brian Banning, CEO

Welcome to the Sacramento InfraGard Members Alliance newsletter!

Recently, the InfraGard Pacific Region Presidents held a two-day summit in San Diego, CA. Attendees from Hawaii and mainland chapters as far away as Idaho, Alaska and Arkansas met and shared best practices. It's interesting to see how different chapters approach things, each reflective of their own regional culture, but grounded in protecting America and the people in it.

That exchange of ideas produced some fantastic prospects that may change the professionalism of our chapter with revisions to administrative non-profit business practices, sponsorship and the sector chiefs' programs.

Several of your Operating Committee members volunteered half of their weekend day to engage in some Strategic Planning. We were fortunate enough that the incredibly experienced Mark Morgan from StratEx Advisors and author of two books on strategic planning joined us to facilitate the meeting and guided us on our first steps of professional strategy planning. A huge THANK YOU to Mark and StratEx!

One strategic goal we identified is to increase information sharing by better serving the membership that isn't in Sacramento. Our chapter covers one of the largest districts in the country, stretching from the Oregon border to Bakersfield, containing almost 8 million people. While still in the formative stages, one tactical change to achieve that strategic goal you should see this fall is the digitization of our training meetings, either as webcasts for remote viewing or a podcast style storage mechanism.

Continued...

A Review of the 2nd Quarterly Meeting

A wonderful turnout at the May 17th, 2017 Quarterly Meeting focusing on the **Health, Financial and Cyber Sectors of our critical infrastructure.** Speakers included:

- ⇒ ***Single Citizen ID Across All Services the State Delivers*** - William (Bill) Harrod, Cyber-Security Advisor for *CA Technologies' Public Sector Security practice*
- ⇒ **Healthcare Emergency Management + Partnerships = Improved Resiliency** - Kristina Freas, CEO, *Freas Emergency Management Group* & Cheri Hummel, *California Hospitals Association*
- ⇒ **CA Cyber Center Briefing** - Colonel Keith Tresh, *Commander, Cal SEC*
- ⇒ **San Bernardino Active Shooter – Domestic Terrorism with an International Affiliation -** Lieutenant Mike Madden, San Bernardino's Public Information Officer & Community Affairs Division Manager*, San Bernardino PD*

Presidents Message Continued

InfraGard exists to enhance and facilitate information sharing between the FBI and the private sector to better ensure Homeland Security and the safety and security of our Nation. I thank you for being in this organization because your individual membership increases the organization's ability to do that.

In closing, thank you to the FBI, all volunteers involved with InfraGard, sponsors, and presenters. And, heartfelt congratulations to Kimberly Pratt, a Sacramento IMA member, who has just been installed as the Executive Director of the InfraGard National Members Alliance!

Responding to Active Shooter and Improved Explosive Devices

DHS Hometown Security: Tools to Help Your Community Prepare - Through the Hometown Security Initiative, DHS provides free tools and resources to communities because the Department recognizes that communities are the first line of defense in keeping the public safe and secure. DHS encourages businesses to connect, plan, train, and report. Applying these four steps in advance of an incident or attack can help better prepare businesses and their employees to proactively think about the role they play in the safety and security of their businesses and communities. Find more at:

https://www.dhs.gov/hometown-security

InfraGard Board of Directors and Operating Committee

The Sacramento IMA holds regular meetings and provides members with a forum for information sharing within a secure environment, while focusing on protecting the critical infrastructure of Sacramento and surrounding areas.
The members of the Sacramento IMA are part of a national network of FBI-vetted volunteers who are Subject Matter Experts (SME) for critical infrastructure in one or more critical sectors. It provides a trusted forum for the real-time exchange of information, training, and expertise related to the protection of critical infrastructure.

FBI Sacramento

FBI Sacramento
2001 Freedom Way
Roseville CA 95678
916-746-7000

2017-2018 Operating Committee

Brian Banning
President & CEO

Doc Dochtermann
Chief Operating Officer

Howard Duck
Secretary

Glynn Davis
Treasurer

EOC DELEGATE ASSIGNMENTS

Brian Banning
Program Chair

Robert Barrow
CCIC/RTAC Liaison

Stephanie Cervantes
Membership & Strategic Plan Chair

Ria de Grassi
Food & Ag Sector Chief

Doc Dochtermann
Information / Communications

Howard Duck
Sector Chief Program Chair

Dennis Garton
Northern Area Representative

Martin Jeppeson
At-Large Delegate / Planning Cmte

Gary Quisenberry
Southern Area Representative

Rami Zreikat
At-Large Delegate

2017-2018 Board of Directors

Outside Directors at-large

Scott Seymour
Former CEO Aerojet

Chris Gallo
Director E & J Gallo

Jim "Mac" McIntosh
CEO GEOGENCO, LLC

Malcolm Harkins
Global Chief ISO, Cylance Corp.

Ralph Hexter
Provost, Exec Vice-Chancellor UC Davis

Vacancy

IMA Internal Directors (inclusive of Officers)

Brian Banning
IMA President & CEO

Doc Dochtermann
IMA Chief Operating Officer

Howard Duck
IMA Secretary

Glynn Davis
IMA Treasurer

Robert Barrow
EOC Director at-large

Advisory Committee

- Alturi, Srinivas
- Armstrong, Gary
- Bailey, Tim
- Chow, Bob
- Hackmann, Jonathan
- Kendricks, Walter
- Mohr, Selby
- Orlove, Jack
- Pratt, Kimberly
- Sellner, Joe
- Stovall, Larry
- Ulrich, John
- Woods, Andrew

InfraGard Membership ALERT

Sacramento InfraGard members are reminded that is necessary to log into the national portal at least every 90 days to maintain active membership.

InfraGard.org

Visiting this chapter webpage does not serve to keep your membership active.

New Website!!

If you haven't already visited , check out the new Sacramento InfraGard Members Alliance website:

InfraGard-Sacramento.org

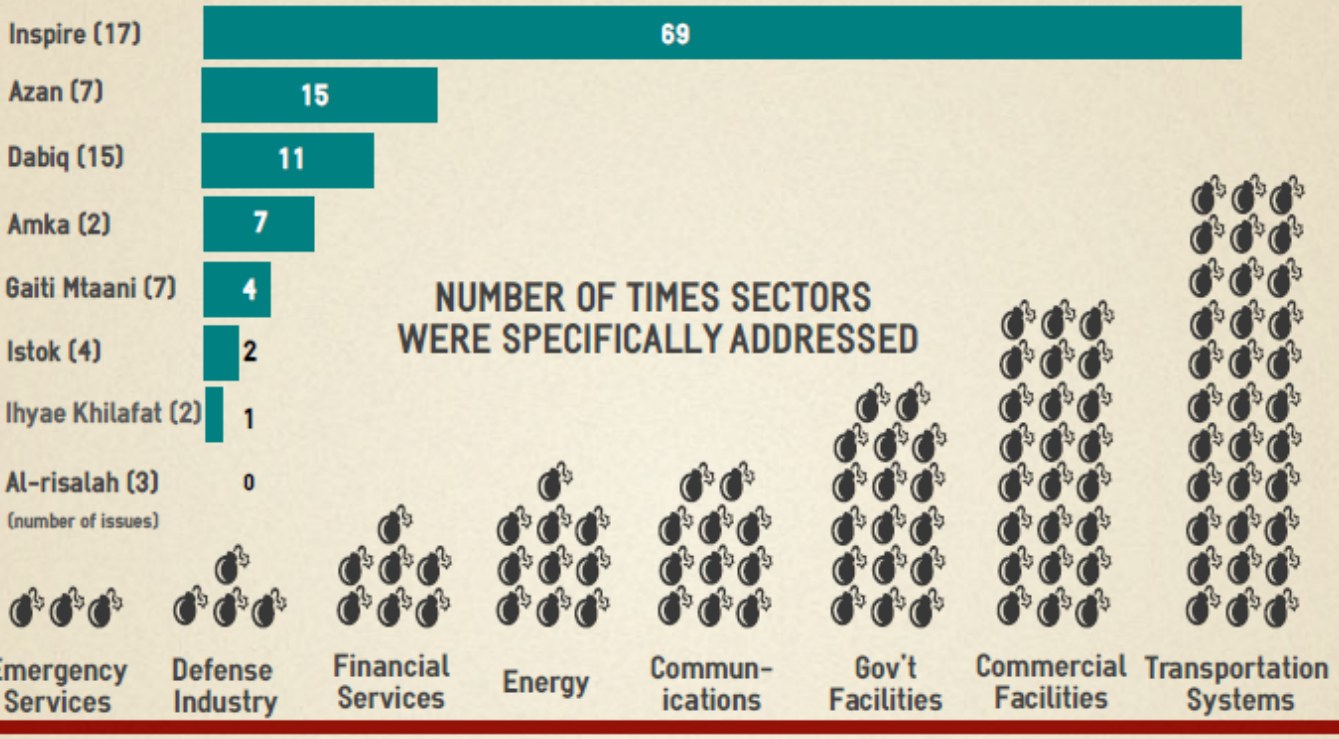
UNCLASSIFIED

EXTREMIST E-ZINE ATTACK SUGGESTIONS

This product informs infrastructure owners/operators of what might be targeted by Islamic extremists for risk management decision making.

In a comparative review of selected e-zines from a critical infrastructure (CI) protection perspective, it is immediately apparent that AQAP's Inspire is dramatically more involved in trying to operationalize jihadists than other publications studied. Inspire comprises only 29% of the e-zine issues but provides 63% of attack suggestions and methodology instruction. AZAN, the next closest e-zine in this category, had 12% of the issues researched and only 14% of the targeting comments.

WHICH PUBLICATIONS ARE MAKING THE MOST SUGGESTIONS?



SUGGESTED METHODS

Small arms and explosives were referenced most

Using aircraft, arson, vehicle ramming, edged weapons, and chemicals were emphasized

CRITICAL INFRASTRUCTURE SECTORS AND METHODS SUGGESTED?

Jihadist e-zines disproportionally suggest attacking 3 of the 16 CI sectors: transportation, commercial facilities, and government facilities, accounting for 68% of their suggestions. This CI focus roughly aligns with the Global Terrorism Database (GTD)* records for worldwide attack sites and methodologies used since 2010. While complex (explosive/armed) attacks against CI may produce the highest consequences, low capability HVEs are likely to use simpler attacks against personnel instead of the actual infrastructure.

For information on countermeasures please visit: US DHS.

Notes: E-zines are magazines published only electronically. The e-zines are published by the following: Ihayae Khilafat by Jammaat-ul-Ahrar, Amka by Al-Muhajiroun, al-risalah by Al-Nusrah, Azan by Taliban, Gaidi Mtaani by Al-Shabaab, Dabiq and Istok by ISIL, and Inspire by al-Qa'ida. Research was done using the English version of the listed ezines (Istok was researched in Russian) and no social media was taken into account. Inspire produced a Pocket Guide in the Spring of 2013 which was a compilation of some of their previous issues, therefore it was not included to avoid double-counting. Attack suggestions are attributed to an issue when an attack against critical infrastructure was included in either words or images. Not included in the compilation by sector: 1) Inspire advocates following executives to their residence where security is lower and killing them there. This applies mostly to executives whose killing could have a significant economic impact. 2) ISIL suggests targeting military, police, and intelligence services in the countries opposing their efforts in Syria; particularly those from the US, UK, France, Canada, Germany, and Australia. Note that each of these countries have already been attacked by ISIL inspired HVEs.

* National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd

UNCLASSIFIED

12 January 2017

Save the Date…

Active Shooter Training June 14— 8am-12pm, Location: 3720 Dudley Blvd. McClellan Park, CA 95652

GETS/WPS for InfraGard Members

The Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) are emergency communications services offered by the United States Department of Homeland Security.

They essentially prioritize your communications traffic over nonmembers when service is overwhelmed by high message traffic during disaster response and recovery.

There is an application process and InfraGard members are all eligible for these services.

GETS is a free service designed to support national leadership; federal, state, local, tribal and territorial governments; and other authorized national security and emergency preparedness users. Enrolled members get a telephone calling card.

WPS is an easy to use add on feature subscribed to a per cell phone basis. WPS calls receive priority over normal cellular calls. WPS is added to your monthly wireless bill (10$ activation + $4.50 per month + .75 cents per minute.

To apply for GETS and/or WPS please contact:
Mr. Jaime Chanaga, National GETS/WPS Coordinator
GETS@InfraGardMembers.org
(212) 203-3925

Cyber Hygiene Tips

By Rusty Sailors
Chairman and CEO, LP3 SecurIT, and Chairman, Protecting Tomorrow

Cyber security is a business problem, not a technical problem – you have to solve it as one. Hackers run successful international enterprises, leveraging an agile and adaptable business model. They benefit from your lack of attention to cyber security and poor investment in protecting your data. Did you know you're twice as likely to be successfully hacked then to get in an auto accident? Yet many small to medium-sized businesses are not wearing a cyber security seat belt. The following cyber hygiene tips will give you a head start on the road to cyber safety.

Email and Phishing

- Automatically delete anything that looks out of the ordinary.
- Phishing is one of the most effective means to gain access to your account. If the email looks like it's from someone you know, give them a call or send a text to make sure – they'll be glad to hear from you.
- Often the sender will have gathered some basic information about you and include it in the email you receive so it appears legitimate.

CONTINUED...

Banking, Public Computers and Free WiFi

- When using online banking services, make sure the sites you navigate to are secure.
- One quick clue to determine whether a website is safe is if the URL begins with “https://.”
- Look for the padlock icon at the bottom of your browser, which indicates the site uses encryption.
- Type web site URLs directly into the address bar. Do not follow links – go directly to the known web site for your bank or other institution.
- If at all possible, don’t use public computers – someone can log your info!
- Never use free public WiFi – it’s worth it to use your phone’s hot spot.
- f you have to use a public computer, such as one at a hotel, never enter your personal information.

Social Networks

- Develop a social media policy for your organization.
- f you want to share pictures of your travel, share them after you return.
- Choose a strong password that you change often.
- Take the time to set your privacy settings to control who can see what.
- Sharing personal information online can give hackers the information they need for very successful spearphishing.
- Always think carefully about any information you choose to share online.

Passwords

- Many people choose a password that's easy to remember – like an address, pet's name or special date – and use it over and over again.
- These are easy to find through the weakest accounts, and attackers try these first because they can gain access to many different valuable accounts.
- To protect your passwords online, follow these tips: Make sure it's a minimum length of eight characters.
- Include at least one character that isn't a letter or number – e.g. a symbol.
- Be creative. Use the first letter of each word of a memorable sentence or phrase, then make it even tougher by changing some of the letters to numbers (e.g. use a "3" to replace an "e").
- Consider an odd passphrase you will always remember
  “Old dogs eat blue ice cream” and modify it to something like:
  “O1ddogs3@tblue!cecream” – just a few changes you can remember
- Choose a password manager – then use the complex passphrase to access the password manager.
  The password manager creates complex passwords for your ac counts.
  It enters the credentials or password for you.
  The likelihood of reputable password managers getting hacked is minimal compared to someone finding the same password you use all the time.
- Choose odd, but memorable answers to security questions:
  What was the make of your first car: “blue”
  What high school did you attend: “cold”