Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

**February 2013**

# Industry Alert: Recent DDoS Attacks

## FS-ISAC Summary

The Financial Services Information Sharing and Analysis Center (FS-ISAC) issued a proprietary alert regarding the recent and increased distributed denial of service (DDoS) attacks launched against multiple and smaller financial institutions.The advisory provides an overview of the attacks, as well as suggested advance mitigation strategies, key indicators, and information on escalation and reporting.

Members of the FS-ISAC can access the advisory via **www.fsisac.com**.

Members of the American Bankers Association can access the advisory, in addition to tips for communicating with customers about these events, via the **ABA's Fraud & Security Solutions** site.

## OCC Advisory

The Office of the Comptroller of the Currency (OCC) also issued an advisory for financial institutions and technology service providers, describing the attacks and outlining recommended mitigation efforts and responses to include:

- Ensuring sufficient staffing for the duration of DDoS attacks in conjunction with pre-contracted third-party servicers that can assist in managing the Internet-based traffic flow;
- Ensuring that incident responses effectively involve the appropriate personnel across multiple lines of business and external partners;
- Conducting due diligence reviews of service providers, such as ISPs and Web-hosting servicers, to ensure they have taken the necessary steps to identify and mitigate the risks stemming from potential DDoS attacks;
- Identifying and appropriately considering new and evolving threats to online accounts and adjusting customer authentication, layered security, and other controls as appropriate in response to changing levels of risk; and
- Reporting DDoS attacks to law enforcement authorities, notify their supervisory office, and file a Suspicious Activity Report (SAR) if the attack affects critical information including customer account information or damages, disables or otherwise affects critical systems of the bank.

The advisory also reiterates warnings that these attacks could be used in conjunction with attacks designed to facilitate fraudulent wire transfers. **Read the advisory**.

INSIDE THIS ISSUE

# Cybersecurity News

## Executive Order: Improving Critical Infrastructure Cybersecurity

On February 12, President Obama issued an **executive order** intended to safeguard the nation's critical infrastructure against cyberattacks, urging Congress to act quickly and pass legislation that gives government a greater capacity to secure networks and deter attacks.

The executive order gives the federal government responsibility for working with private companies to develop voluntary cybersecurity standards, in which the National Institute of Standards and Technology (NIST) will take the lead in issuing a preliminary version of the framework within 240 days of the executive order. It also designates the Treasury Department as the financial services industry's sector-specific agency.

Members of the FSSCC will continue to monitor and report on further developments stemming from the executive order.

## BRT Report: More Intelligent, More Effective Cybersecurity Protection

A new **report** from The Business Roundtable acknowledges the integral role that information sharing plays in effective cybersecurity policies in order to combat threats from nation states and other well-funded and highly motivated actors.

To effectively address the risks presented by cybersecurity threats, Business Roundtable (BRT) CEOs have developed a cross-sector approach that encourages:

1. **Robust, two-way information sharing**, with appropriate legal and privacy protections, between government and the private sector to exchange specific threat information to allow both government and business to better secure the nation's cyber assets and mitigate emerging threats in real time.
2. The **development of threat-informed risk management and mitigation methodologies**, including those that increase law enforcement capabilities to disrupt, apprehend and prosecute cyber criminals.
3. **CEO commitment tocybersecurity** which includesinvestments in the infrastructure to receive shared threat information and the integration of cybersecurity threat and risk information into CEO risk management. BRT also calls upon boards of directors, as part of their risk oversight functions, to "continue to periodically review management's business resiliency plans, including cybersecurity, and oversee risk assessment and risk management processes, including those applicable to cybersecurity."

*"Effective information sharing is not only an exchange of threat information but also a robust set of well-structured and regularized policies and processes among the U.S. government, international allies and private-sector entities…However, instead of focusing on information sharing and collaborative risk management, government proposals misdirect scarce resources to compliance-based check-the-box models." – BRT Report*

# Business Resiliency News

### *Resolve to be Ready 2013*

FEMA unveiled their "Resolve to be Ready" initiative for 2013.

This initiative is part of FEMA's Ready Campaign, which provides the public with tools and resources to enhance preparedness for major events.

The campaign encourages the public to:

- be informed about the different types of emergencies that can happen in their area and the appropriate preparedness steps;
- make a family communications plan; build an emergency kit; and
- get involved in community preparedness.

Click **here** for more information, including web banners and campaign logos.


## 2012-2013 Flu Season Information

In a Jan. 11 CNN.com article, an official from the National Institutes of Health stated that, with more than 40 states reporting widespread activity, the U.S. is experiencing what would classically be described as a "flu epidemic."

For information, please see the following:

- Center for Disease Control (CDC) **Flu Activity & Surveillance site**. This site includes weekly and archived situational reports, national and international maps of current flu activity, and more.
- **Flu.gov**. Managed by the U.S. Department of Health and Human Services, this site provides general information about the flu including symptoms and treatment, planning and preparedness, and pandemic awareness. It also provides the Flu Vaccine Finder where users may find a flu vaccine location near them.

## DHS Private Sector Resources Catalog

The U.S. Department of Homeland Security Private Sector Office announced the availability of the *Private Sector Resources Catalog*. The catalog contains information about the various tools and resources provided by DHS to businesses to assist them in preparing for, mitigating the effects of, and recovering from a major event or disaster.

Sections that may be of particular interest to those in the financial services sector include: DHS department-wide resources and key contacts; resources for safeguarding and securing cyberspace such as cybersecurity assessment tools, incident and technical resources, and software assurance programs; and a business resiliency section that highlights resources for business, community and personal preparedness, emergency communications, and more. **Read more**. **Access the report**.

## FEMA Disaster Apps

FEMA announced the availability of apps to provide users with:

- disaster safety tips,
- interactive lists for storing emergency kit and emergency meeting location information, and a
- map with open shelters and open FEMA Disaster Recovery Centers (DRCs).

The app is free to download through users' smartphone provider's app store:

- **Android devices**
- **Apple devices**
- **Blackberry devices**

# Business Resiliency News, continued

## National Severe Weather Preparedness Week is March 3-9, 2013

During National Severe Weather Preparedness Week, scheduled from March 3-9, 2013, the Federal Emergency Management Agency (FEMA) and the National Oceanic and Atmosphere Administration (NOAA) emphasize the need for individuals, families, businesses, and nonprofits to prepare emergency plans, and to know what to do before severe weather strikes.

The goals of National Severe Weather Preparedness Week are to:

- Inform the public about the severe weather hazards in their locality;
- Provide information that can be used to prepare individuals and communities for severe weather events; and
- Motivate individuals and communities to take actions that will prepare them in the event of a severe weather disaster and to share their preparedness steps with others. These actions can save lives anywhere - at home, in schools, and in the workplace before tornadoes, thunderstorms, and other severe weather strikes.

Companies wishing to participate in National Severe Weather Preparedness Week and educate consumers on how to protect themselves can download and customize the following templates:

- **National Severe Weather Preparedness Week Talking Points**
- **Social Media Tools**
- **Press Release**
- **OpEd Template**

More information on tornadoes and severe thunderstorms is available at www.weather.gov and ready.gov/severe-weather.

## Earthquake App


The American Red Cross has an app to help notify and prepare the public in the event of an earthquake. Features include:

- Step-by-step instructions on what to do before/during/after an earthquake, even if no data connectivity;
- Notifications from the United States Geological Survey (USGS) when an earthquake occurs;
- Customizable “I’m Safe” alerts for Facebook, Twitter, email and text;
- Information about open Red Cross shelters in your area
- A strobe light, flashlight and audible alert functions; and more.

Call "**REDCROSS" (**73327677) from your mobile phone to receive a downloadable link or download it directly from the **iTunes** or **Google Play** app stores.

# FSSCC News and Committee Information

## FSSCC Leadership

***Chair:***
*Charles Blauner, Citi*

***Vice Chair:***
*Jim Wells,*
*The Financial Services Roundtable*

***Secretary:***
*Jim Devlin, Citi*

***Operations Manager*:**
*Shirley Burt, Citi*

**Committee Chairs**

***Communications:***
*Heather Wyson,*
*American Bankers Association*
*and*
*Anuj Goel, Citi*

***Policy:***
*Doug Johnson,*
*American Bankers Association*
*and*
*Gary Owen, Goldman Sachs*

***Research & Development (R&D):***
*Dan Schutzer, BITS*
*and*
*Bob Blakley, Citi*

***Threat & Vulnerability Assessment***
*John Carlson, BITS*
*and*
*Byron Collie, Goldman Sachs*

***FS-ISAC Business Resiliency***
*Karl Schimmeck, SIFMA*
*and*
*Mike Tracy, Bank of America*

## FSSCC Submits Comments on DHS Draft 2012 National Risk Profile

On Jan. 11, the FSSCC submitted a comment letter in response to the Department of Homeland Security's draft 2012 National Risk Profile (NRP). The letter outlined the following recommendations to assist the NRP in meeting the objective to inform the risk management decisions of policy and budgetary decision makers and critical infrastructure partners:

- Provide a risk profile and a prioritization of likelihood of impact
- Address threats to businesses as the ultimate owners of critical infrastructure
- Identify risks that are unique to specific sectors

The letter highlighted several unsubstantiated statements regarding risks contained in the report and recommended that future versions include "reliable and credible statistics on cyber and physical incidents."

Members of the FSSCC's Policy and Threat and Vulnerabilities Committees participated in the development of this comment letter.

## Policy Committee

Gary Owen, Vice President, Information Risk, at Goldman Sachs has been named to serve has a co-chair of the Policy Committee. Working with co-chair Doug Johnson, ABA, Gary will lead the subcommittee in their continued efforts to:

- Engage with members of Congress concerning cyber security legislation through participation in a number of House and Senate staff briefings to outline **FSSCC cyber security policy recommendations**;
- Assist the Threat and Vulnerability Committee with the development of a process for the identification of financial sector critical infrastructure;
- Evaluate and respond to proposed cybersecurity Executive Order and HSPD-7 rewrite; and
- Evaluate and respond to proposed Senate cybersecurity legislation.

## Research & Development Committee

In addition to managing the Financial Institution-Verifying Identity Credentials Service (FI-VICS) project, which will prototype and evaluate the value and effectiveness of the new identity proofing verification process based on state drivers' license information and develop an open standard interface for direct verification of identity credentials, this group will update the following:

- FSSCC R&D agenda; and
- Subject Matter Advisory Response Team (SMART) Program. The objective of the SMART Program is to improve interactions between FSSCC members and R&D community with respect to influencing, identifying and extracting value of relevant government funded research and programs that align with the challenges faced by the financial industry.

# FSSCC News and Committee Information, continued

## Threat & Vulnerability Assessment

This Committee, in conjunction with the Policy Committee, developed a comment letter in response to the draft 2012 National Response Plan. The letter, submitted to DHS on Jan.11 recommends that future versions include credible and reliable statistics, as well as:

- Provide a risk profile and a prioritization of likelihood of impact
- Address threats to businesses as the ultimate owners of critical infrastructure
- Identify risks that are unique to specific sectors

## FS-ISAC Business Resiliency Committee *(formerly the Resiliency Management Committee)*

The Financial Services Sector Coordinating Council's (FSSCC) Resiliency Management Committee has now merged with the FS-ISAC's Business Resiliency Committee, with the latter name surviving. These complementary committees have joined together to Organize, direct and support the capabilities of the FS-ISAC to deliver business continuity planning, disaster response and physical security services that are of value to its members.

## About the FSSCC

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), established in 2002, is the sector coordinator for Financial Services for the protection of critical infrastructure, focused on operational risks.

The FSSCC's mission is supported by Homeland Security Presidential Directive #7, which directs government agencies to identify and protect critical infrastructure.

The FSSCC works closely with the Treasury as its designated Sector Specific Agency (SSA), establishing a strong public-private partnership to maintain a robust sector that is resilient against manmade or natural incidents.

Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of consumers and the country's populace. Click **here** to see a list of the current subcommittees and leaders.

We hope you find the information contained in the newsletter to be helpful in understanding the resources available to protect our industry against physical and cyber threats.

## About this Newsletter

This newsletter is distributed to all trade associations involved in the FSSCC.

Current and previous editions are also made available to the public via the FSSCC website, **www.fsscc.org**.

We hope you find the information contained in the newsletter to be helpful in understanding the current threats and the resources available to protect our industry against physical and cyber threats.

Your feedback is important to us. Please consider participating in **this survey** so we may better tailor future newsletters to suit your needs.