

# United States Computer Emergency Readiness Team

Presentation for the California CISO Lecture Series

Randy Vickers, Director (Acting), US-CERT

February 2010



Homeland  
Security

# Agenda

- Threat Environment
- US-CERT Mission and Response Management
- US-CERT Competencies
  - Collection, Monitoring & Analysis
  - Information Sharing & Coordination
  - Alerts, Warnings, Bulletins & Reports
  - Response & Assistance
- Managing Risks on an Enterprise Basis



# Challenges

## Technological Advances

- Integrated capabilities (mobile devices/social networking)
- Robust personal computing capability

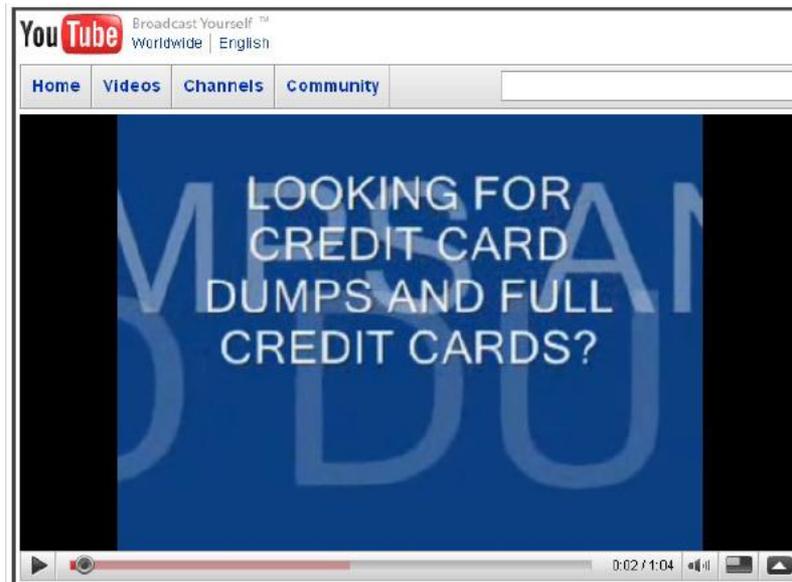


## Customizations

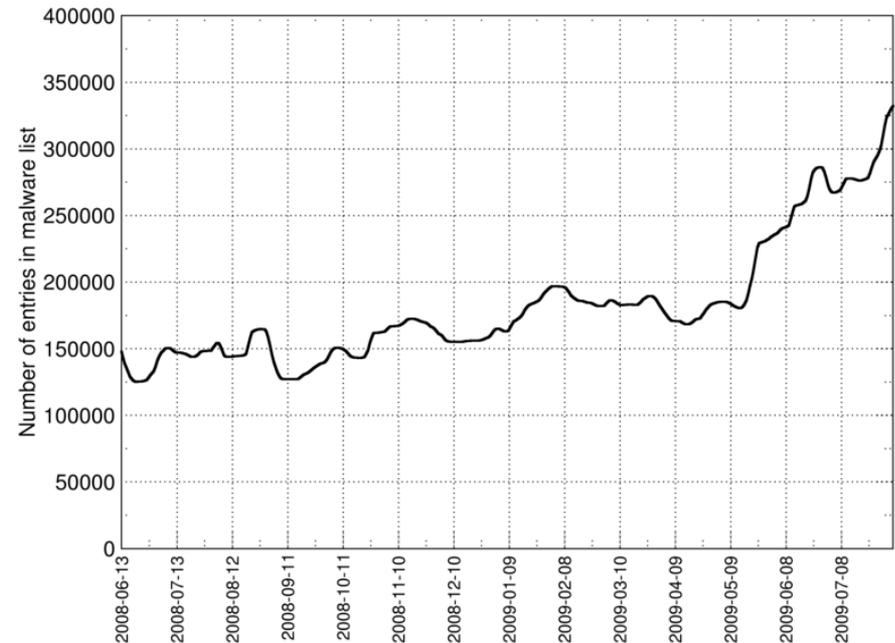
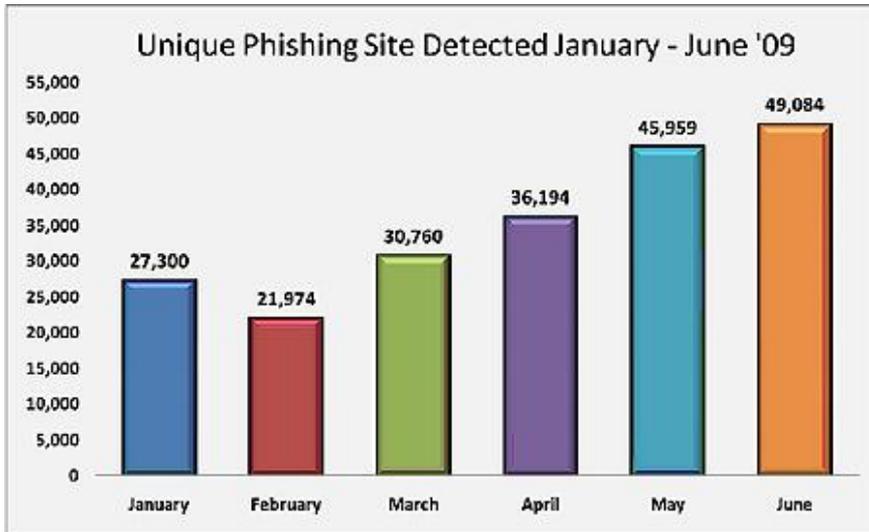
- Low detection rates
- Uncoordinated border factions
- Increased malware “noise”

## Threat Specialization

- Phishers
- Spammers
- Malware Authors
- Mules



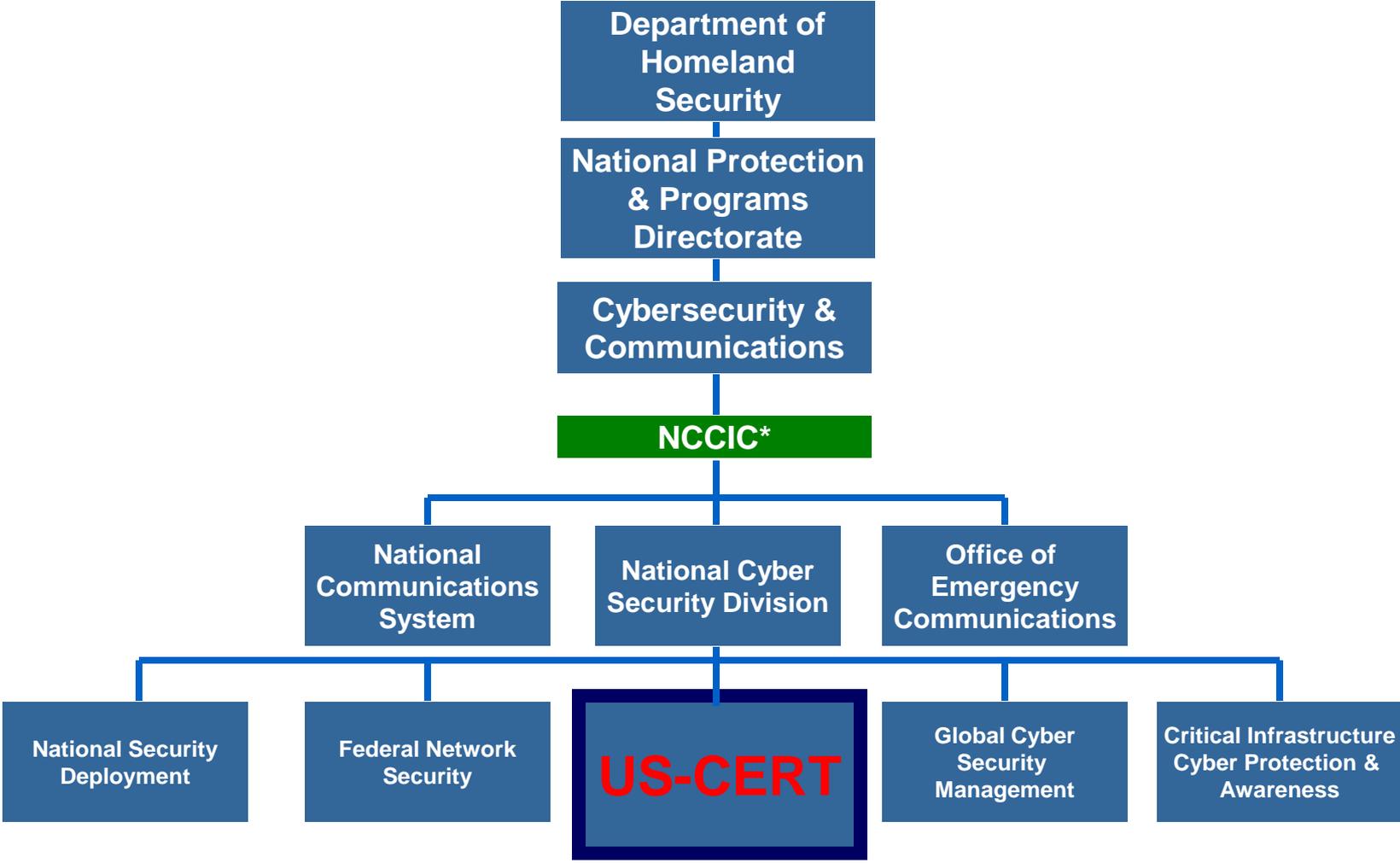
# Emerging Cyber Security Threats



- **Social Engineering** - Phishing/Spear Phishing
- **Web Surfing** - Social Networks (Facebook, MySpace, YouTube, etc.)
- **Activist Influenced Criminal Activity** - Examples: Lithuania and Estonia
- **Increase in Zero Day Vulnerabilities**
- **More Collaboration Between Groups** - Sharing tools (tools for sale on auction sites, hacker forums)



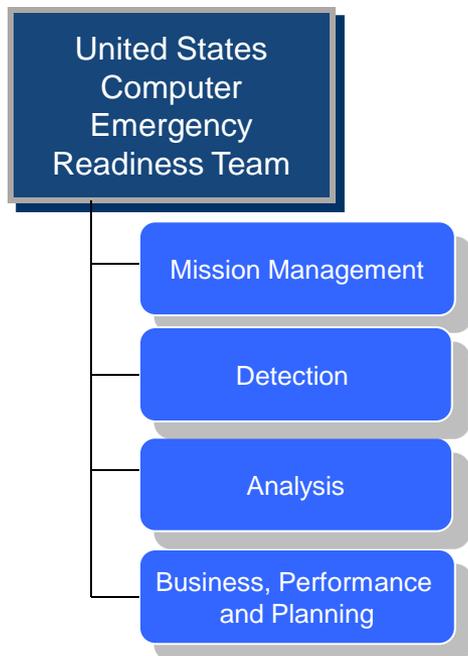
# Organizational Chart for DHS



Homeland Security

\* Currently the NCCIC is not an organizational unit but rather a combined watchfloor

# US-CERT Mission



- Lead and coordinate efforts to improve the Nation's cybersecurity posture, promote cyber information sharing, and manage cyber risks to the Nation.
  - Analyze and reduce cyber threats and vulnerabilities,
  - Disseminate cyber threat warning information,
  - Coordinate with partners and customers to achieve shared cyber situational awareness of the Nation's cyber critical infrastructure,
  - Provide response and recovery support for national assets, and
  - Advise on national-level cybersecurity policy and guidance.



# Response Management

Activities are based on the nature and severity of the threat, vulnerability or incident and US-CERT focuses on tracking impacted parties' progress towards resolving the issue:

- Threat: Analysis of information collected by US-CERT and its partners in order to understand the threats: their identity, their intent and their capabilities.
- Vulnerability: Prioritization of exploitable weaknesses in order to assess potential impact and/or cyber risk to the Nation.
- Attack Detection: Identification of attack activity that exists in complex, multi-agency, multi-platform environment.
- Mitigation: Identification, dissemination and implementation of strategies to contain or resolve risks and attacks.
- Reflection: Collaboration with other organizations to refine federal information security policy and guidance and provide organizations with more accurate strategies.



**Homeland  
Security**

# Collection, Monitoring & Analysis

- Paired with incident reporting, monitoring and analysis facilitates US-CERT's strategic analysis capabilities in order to maintain situational awareness
- Einstein Monitoring
  - Facilitates strategic analysis to detect behavioral threats
  - Establishes baseline trending for agencies
  - Enables cross-agency analysis to identify large-scale threats and vulnerabilities
- Digital Media and Malware Analysis
  - Improves understanding of current and emerging cyber threats and provides actionable information to aid in protection and response efforts
  - Relies on close ties and trust relationships with other malicious code analysis capabilities



# NCPS

- The National Cybersecurity Protection System
  - A “system of systems” that work together to provide overall capabilities for US-CERT. This includes:
    - Portal: US-CERT maintains a secure portal to facilitate product distribution and enable members to interact in a secure environment
      - Compartments are established based on customer groups (e.g. GFIRST, Critical Infrastructure, U5, Control Systems, ISACs)
      - Members must be approved by government compartment ‘owner’ in order to access and be able to collaborate within the compartment
      - Members access portal through two-factor authentication
    - Einstein (E1, E2, E3)
    - SIEM (Security Information and Event Management)

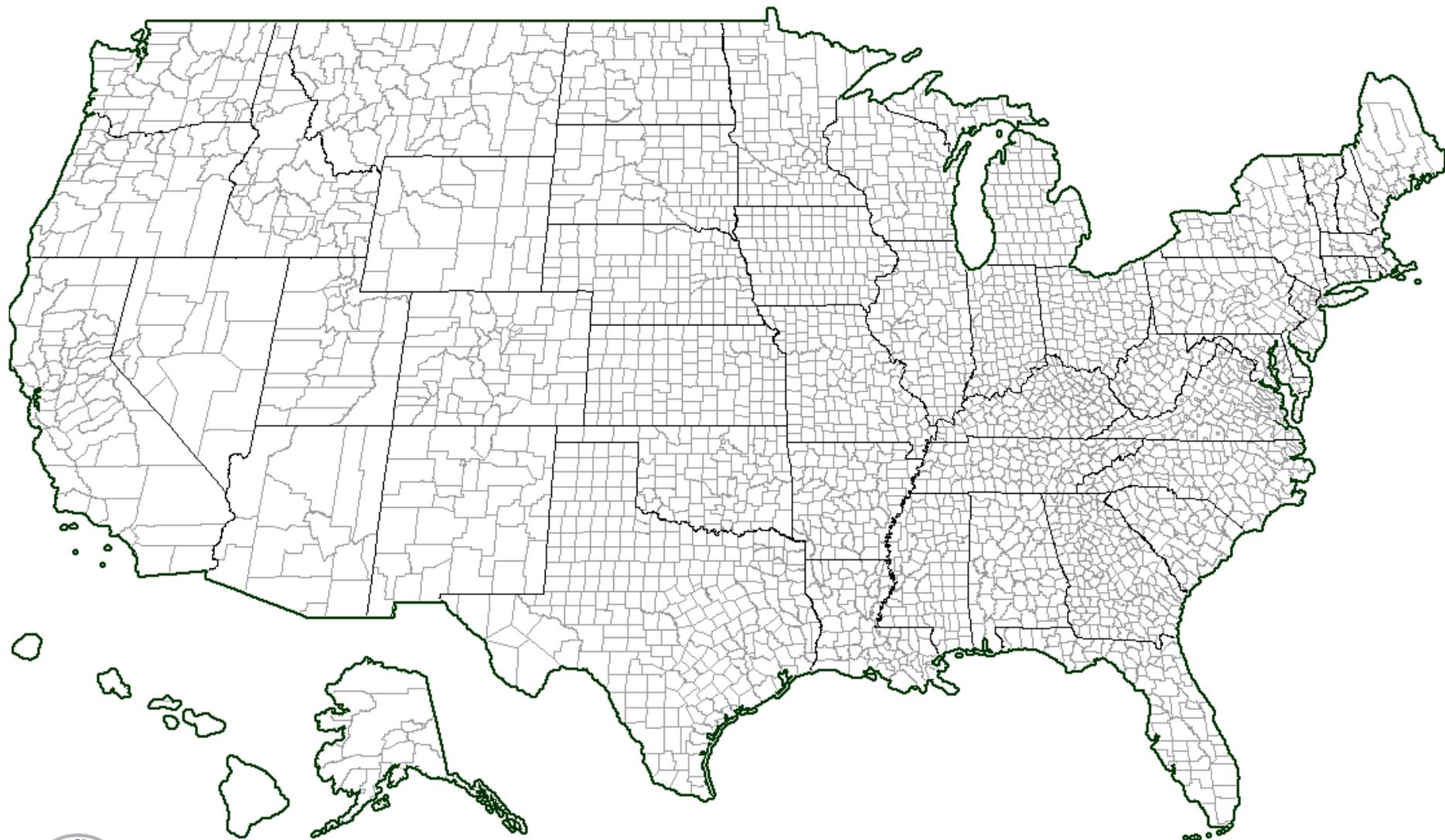


# Information Sharing & Coordination

- US-CERT gathers information on incidents affecting the Nation's cyber infrastructure groups and coordinates with each of these groups in different capacities as deemed necessary
- Interactions consist of two-way information sharing to improve overall situational awareness
- US-CERT must rely on coordination and collaboration with a number of communities of interest:
  - Federal Entities
  - State & Local Governments
  - Law Enforcement
  - Intelligence
  - Corporations
  - International Governments
  - ISACs
  - Control Systems Security Center (CSSC)
  - Media & Public Affairs
  - Software & Hardware Producers
  - General Public



# Working with State, Local and Tribal



**Homeland  
Security**

# U.S. Critical Infrastructure

| Sector-Specific Agency   | Critical Infrastructure/Key Resources Sector  |
|--|---|
| Department of Agriculture <sup>1</sup><br>Department of Health and Human Services <sup>2</sup> | Agriculture and Food  |
| Department of Defense <sup>3</sup>   | Defense Industrial Base   |
| Department of Energy   | Energy <sup>4</sup>   |
| Department of Health and Human Services  | Public Health and Healthcare  |
| Department of the Interior   | National Monuments and Icons  |
| Department of the Treasury   | Banking and Finance   |
| Environmental Protection Agency  | Drinking Water and Water Treatment Systems  |
| Department of Homeland Security<br><i>Office of Infrastructure Protection</i>                  | Chemical<br>Commercial Facilities<br>Dams<br>Emergency Services<br>Commercial Nuclear Reactors, Materials,<br>and Waste |
| <i>Office of Cyber Security and<br/>Telecommunications</i>                                     | Information Technology<br>Telecommunications  |
| <i>Transportation Security Administration</i>  | Postal and Shipping   |
| <i>Transportation Security Administration,<br/>United States Coast Guard<sup>5</sup></i>       | Transportation Systems <sup>6</sup>   |
| <i>Immigration and Customs Enforcement,<br/>Federal Protective Service</i>                     | Government Facilities   |



# Government Forum of Incident Response and Security Teams (GFIRST)

A government information-sharing effort focused on daily information exchange among technical operators across different incident response teams that represent the defense, intelligence, law enforcement, and federal civilian agency communities.

- Community of 50+ Federal agency Incident Response Teams
- Teams work together to secure U.S. Government networks
- Collaborate during on-going cyber activities for technical analysis and information sharing amongst the Government
- State Cyber Security Teams are now GFIRST members and will be a valuable partner to fusion centers to communicate appropriate developments they learn through this information sharing community



**Homeland  
Security**



# Alerts, Warnings, Bulletins & Reports

- National Cyber Alert System is a cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats
  - **Cyber Security Alerts** – Provides timely information about security issues, vulnerabilities, and exploits currently occurring
  - **Cyber Security Tips** – Written for non-technical home and corporate computer users, the bi-weekly Cyber Security Tips provide information on computer security best practices
  - **Cyber Security Bulletins** – Written for the technical audiences, Cyber Security Bulletins provide bi-weekly summaries of security issues, new vulnerabilities, potential impact, patches, and workarounds, as well as recommended actions to mitigate risk
- Additionally compiles analytical information notices specific to US-CERT's communities of interest



# Public Information Dissemination

## National Cyber Alert System

### Mailing Lists and Feeds

#### Subscribe to a mailing list

US-CERT offers mailing lists and feeds for a variety of products including the National Cyber Alert System and Current Activity updates. The National Cyber Alert System was created to ensure that you have access to timely information about security topics and threats. To make it easier for you to receive the information, US-CERT offers five mailing lists that you can you can subscribe to. You may choose one or more of the following types of documents:

- Technical Cyber Security Alerts
- Cyber Security Bulletins
- Cyber Security Alerts
- Cyber Security Tips
- Current Activity

To learn more or subscribe, visit the [subscription system](#). If you're having trouble subscribing, read the [FAQ](#).

#### Feeds for some of our security documents

You can view US-CERT security documents on our web site or use our [RSS](#) and [Atom](#) feeds. Some of these feeds can also be [added to your My Yahoo! page](#) if you have one.

| Document Type   | Feed                                     | My Yahoo  |
|---|--|---|
| <b>Technical Cyber Security Alerts</b><br><a href="http://www.us-cert.gov/cas/techalerts/">http://www.us-cert.gov/cas/techalerts/</a> | <a href="#">RSS</a>                      | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |
| <b>Cyber Security Alerts (non technical)</b><br><a href="http://www.us-cert.gov/cas/alerts/">http://www.us-cert.gov/cas/alerts/</a>   | <a href="#">RSS</a>                      | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |
| <b>Cyber Security Bulletins</b><br><a href="http://www.us-cert.gov/cas/bulletins/">http://www.us-cert.gov/cas/bulletins/</a>          | <a href="#">RSS</a>                      | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |
| <b>Cyber Security Tips</b><br><a href="http://www.us-cert.gov/cas/tips/">http://www.us-cert.gov/cas/tips/</a>                         | <a href="#">RSS</a>                      | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |
| <b>Current Activity</b><br><a href="http://www.us-cert.gov/current/">http://www.us-cert.gov/current/</a>                              | <a href="#">RSS</a> <a href="#">ATOM</a> | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |
| <b>Vulnerability Notes</b><br><a href="http://www.kb.cert.org/vuls/">http://www.kb.cert.org/vuls/</a>                                 | <a href="#">ATOM</a>                     | <a href="#">+ MY Y!</a><br><a href="#">Add to My Yahoo!</a> |

Top

**US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Security Publications | Alerts and Tips | Related Resources | About Us | Search US-CERT:  [GO](#) [customize](#)

Information For  
**Technical**

### Welcome to US-CERT

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

#### National Cyber Alert System

For Technical Users

- **Technical Security Alerts** [RSS](#) [MY Y!](#)  
Microsoft Updates for Multiple Vulnerabilities
- **Security Bulletins** [RSS](#) [MY Y!](#)  
Vulnerability Summary for the Week of December 3, 2007

For Non-Technical Users

- **Security Alerts (non-technical)** [RSS](#) [MY Y!](#)  
Microsoft Updates for Multiple Vulnerabilities
- **Security Tips** [RSS](#) [MY Y!](#)  
Shopping Safely Online

#### Current Activity

- [RSS](#) [ATOM](#) [MY Y!](#)
- Apple Releases Security Update to Address Multiple Vulnerabilities in QuickTime
- HP Info Center Software Public Exploit Code
- Microsoft Releases December Security Bulletins
- Active Exploitation Using Malicious Microsoft Access Databases
- Microsoft Releases Advance Notification for December Security Bulletin
- Cisco Releases Security Documents for Vulnerabilities
- Microsoft Releases Security Advisory to Address Web Proxy Auto-Discovery Vulnerability

#### Vulnerability Resources

New and Notable Vulnerabilities

- Apple QuickTime RTSP buffer overflow
- RealPlayer ActiveX playlist import vulnerability
- Apple QuickTime remote command execution vulnerability
- Kerberos code execution vulnerability

Other Resources

- Recent Notes [ATOM](#)
- NVD (National Vulnerability Database)

#### Announcements

- US-CERT Quarterly Trends and Analysis Report, Vol. 2, Issue 4  
This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year 2007 fourth quarter (FY07 Q4).
- FBI Announces Results of Bot Roast II  
FBI's "Operation Bot Roast II" identifies and captures eight individuals responsible for infecting over 1 million compromised computers.
- IT Security Essential Body of Knowledge  
The IT Security Essential Body of Knowledge (EBK) is currently available for public comment. The EBK characterizes the IT security workforce and provides a national baseline representing the essential knowledge and skills that IT security practitioners should have to perform specific roles and responsibilities.

[www.us-cert.gov](http://www.us-cert.gov)



**Homeland Security**

# Constituent Information Dissemination



Lee Rock's last login: January 28, 2010 - 11:17

Compartment:

<--New info, check Compartment pulldown!

- Custom Tools**
- Report an Incident
- Report a Vulnerability
- Virtual Training Environment
- Internet Health Services
- Einstein
- Collaboration Tools**
- Secure Messaging (1052 new)
- Library
- Find Users
- Calendar
- Online Briefings
- Forum Discussions
- Questionnaire Tool
- TaskTrac
- Chat (prev)
- WebPort (1 new)
- Alerts (73 new)
- Portal Search
- My Groups
- Admin Tools**
- Update Profile/Preferences
- Suggestion Box
- Report Problems
- Log Out

**Portal Downtime Notification**  
Portal service will be inaccessible during this time.  
Please save your work and exit the system before  
this time to ensure no data is lost.

**Date:** Sunday, January 31, 2010 **Length:** 6:00am - 10:00am EST



UNCLASSIFIED//FOUO

10:00 UTC 03 Dec 2009

## DHS/US-CERT Daily Unclassified Briefing

### Incident Handling

Incident handling data is derived from tickets submitted to US-CERT from the previous day. Incident categories are defined within the [Federal Incident Reporting Guidelines](#). Incidents labeled as Private Sector are those that did not impact a Federal, State, Commercial, ISAC, or Foreign entity. Private Sector incidents are generally private citizens reporting Phishing and Malware instances to US-CERT.

### Incident Statistics By Sector (358 Total Incidents)

- Private : 123
- ISAC : 0
- Federal : 220
- Commercial : 0
- Foreign : 15
- State/Local : 0

### Threat Levels

**National Threat Advisory:**  
**ELEVATED**

Significant Risk Of Terrorist Attacks

infacon: **GREEN**  
<http://isc.sans.org>



Threat Levels provided by 3rd parties for situational awareness purposes

### Cyber News Resources

- [US-CERT Current Activity](#)
- [CERT Coordination Center](#)
- [National Vulnerability Database \(NVD\)](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#)
- [SANS Internet Storm Center](#)



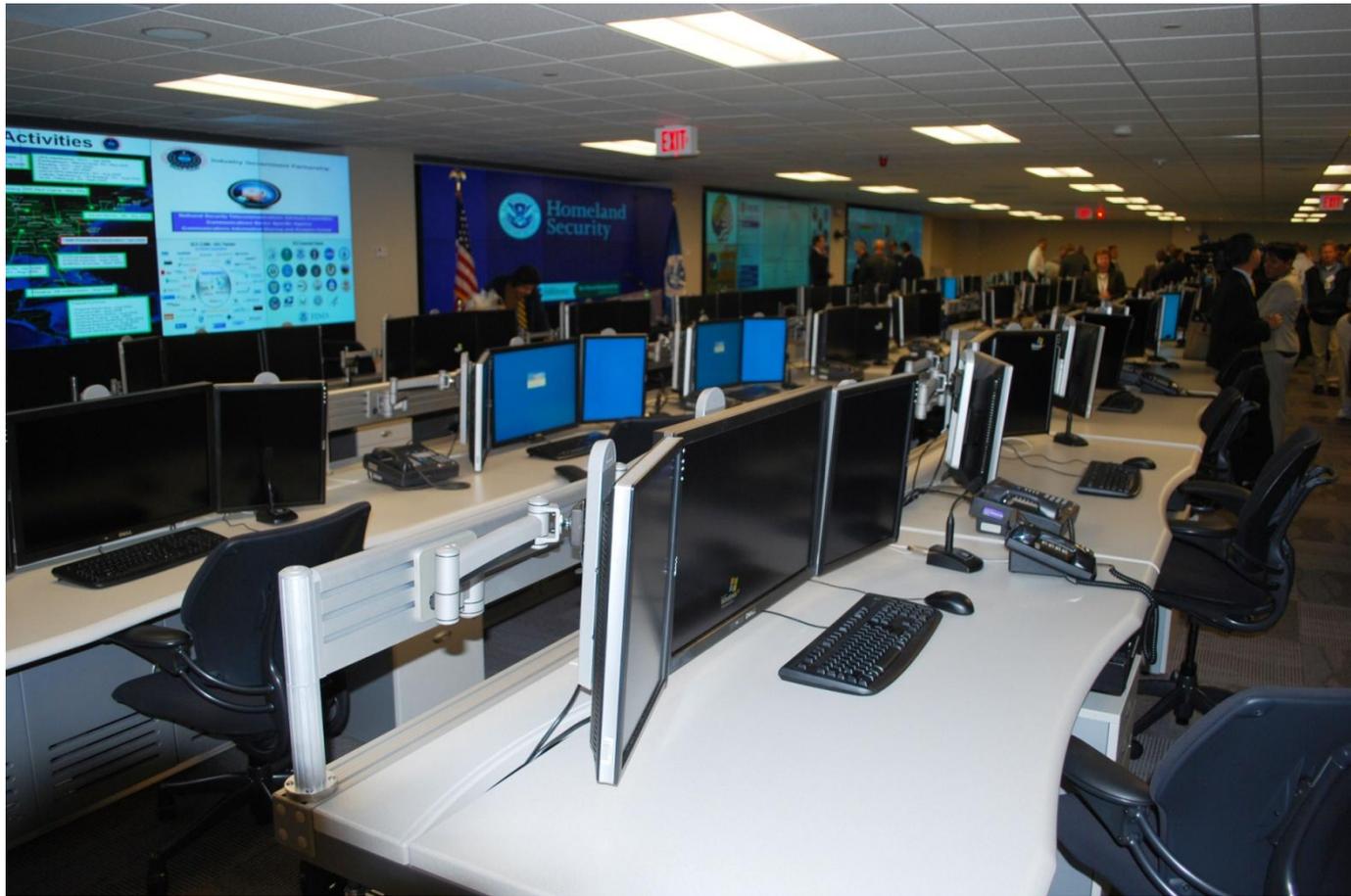
**Homeland Security**

# Response & Assistance

- Activities are based on the nature and severity of the incident and focuses on tracking impacted parties' progress towards resolving the issue
- Dedicated teams ensure appropriate and accurate technical assistance is provided with the right level of subject matter expertise:
  - Digital Media and Malware Analysis
  - Defensive Analysis
  - Mitigation Strategy Development
  - Threat/Attack Vector Analysis
  - Vendor Analysis Coordination
- Deployable teams can provide specialized subject matter expertise required to mitigate or prevent an event from escalating



# National Cybersecurity and Communications Integration Center



Homeland  
Security

# Managing Risks on an Enterprise Basis

- Trusted Internet Connection (TIC) –
  - A multifaceted plan for improving the Federal Government's security posture by significantly reducing the number of external connections including connections to the Internet
- National Cyber Incident Response Plan (NCIRP) -
  - High-level framework for operational coordination among Federal, State, local, tribal and territorial governments, private sector and international partners.
- Cyber Storm III –
  - Largest government-sponsored cyber security exercise of its kind that scenario that produces a global cyber event.
  - Exercises and enable the plans, capabilities, and procedures necessary to ensure the security of the Nation's broad and interdependent cyber infrastructure.



# Contact

- Technical comments or questions:
  - US-CERT Security Operations Center  
Email: [soc@us-cert.gov](mailto:soc@us-cert.gov)  
Phone: +1 888-282-0870
- General questions or suggestions:
  - US-CERT Information Request  
Email: [info@us-cert.gov](mailto:info@us-cert.gov)  
Phone: +1 888-282-0870
  - GFIRST: [gfirst@us-cert.gov](mailto:gfirst@us-cert.gov)
- Information available at <http://www.us-cert.gov>

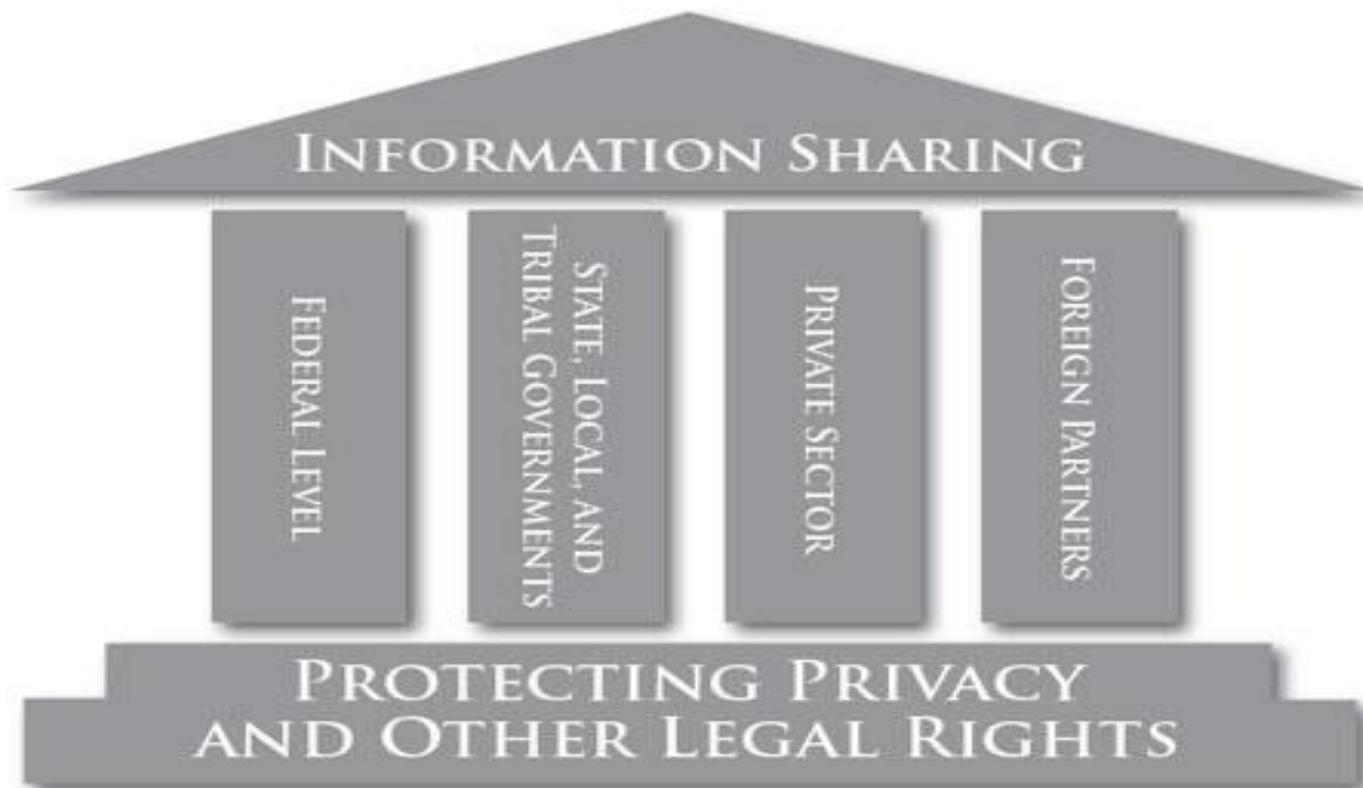


**Homeland  
Security**

# Cabinet Level Agencies



# Privacy



*Foundations of the National Strategy for Information Sharing*



**Homeland  
Security**