



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 1, 2012



ISOAG February 2012 Agenda

- | | | |
|------|---|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Dominion Cyber Security Program | Mark Engels, Dominion |
| III. | Application Testing Using
Random Data Patterns | Bob Baskette, VITA |
| IV. | 2012 General Assembly | Michael Watson, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA
Steve Slight, Jan Weiner,
Casey Rhoton, & Mike Clark, NG |

Information Security Officers Advisory Group (ISOAG)

February 1, 2012

Discussion Topics

- Brief Overview of Dominion
- Dominion's Cyber Security Program
- The Current Landscape
- Threats and Vulnerabilities
- Regulatory and Legislative Update

Discussion Topics

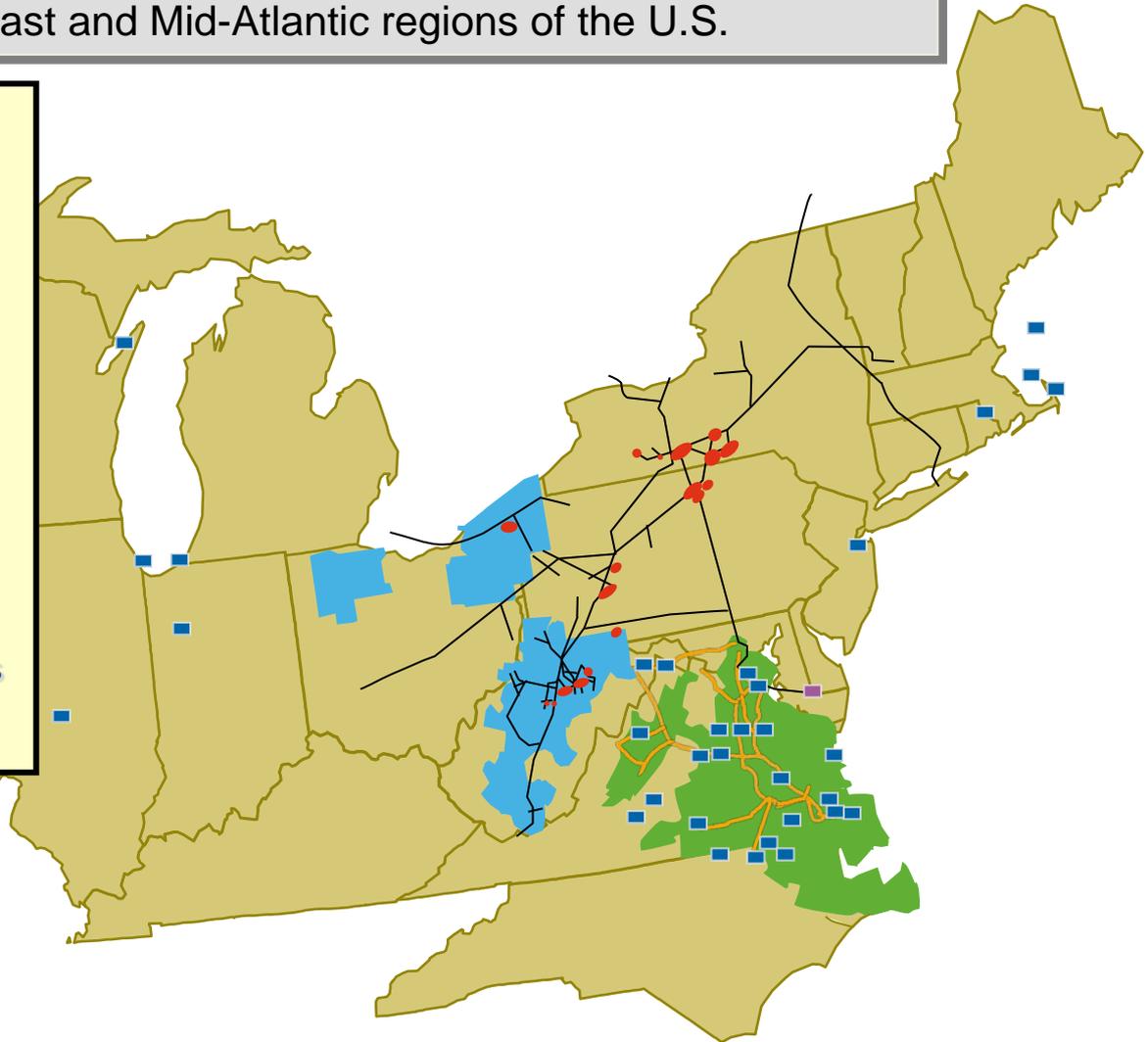
- **Brief Overview of Dominion**
- Dominion's Cyber Security Program
- The Current Landscape
- Threats and Vulnerabilities
- Regulatory and Legislative Update

Dominion Profile

Power and Natural Gas Infrastructure

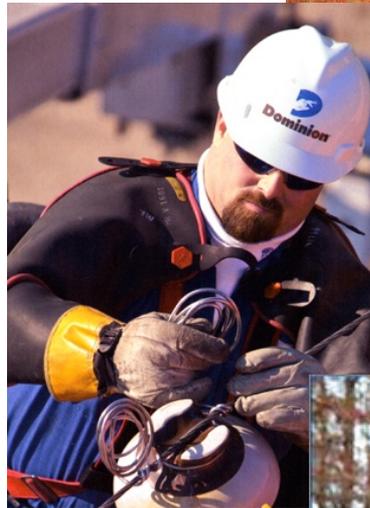
Leading provider of energy and energy services in the Midwest, Northeast and Mid-Atlantic regions of the U.S.

- ~28,000 MW of electric generation
- ~6,300 miles of electric transmission
- 11,000 miles of natural gas transmission, gathering and storage pipeline
- 947 billion cubic feet of natural gas storage operated
- Cove Point LNG Facility
- 2.4 million electric customers in VA and NC
- 1.3 million natural gas customers in OH & WV
- 2.2 million non-regulated retail customers in 15 states



Dominion Virginia Power Profile

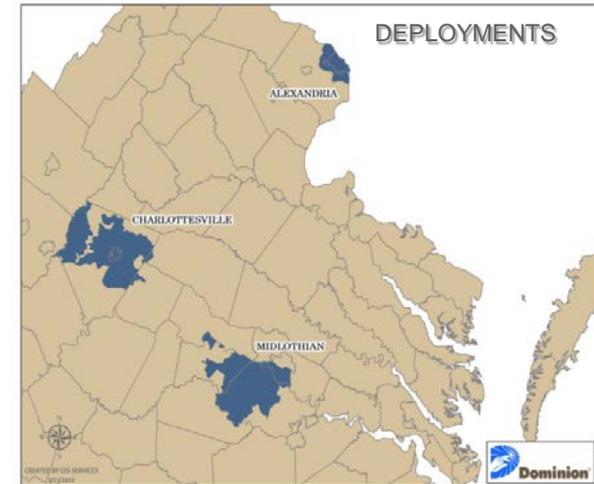
- Serves **2.4 million** franchise electric customers
 - 300,000+ new customers since 2003
- Customers are being served by
 - **56,900** miles of electric distribution lines
 - **6,300** miles of electric transmission lines
- Customer Care Center handling more than **7 million** calls per year
 - Approximately 36% of customer contacts are now self-service
- Dominion Retail serves **2.2 million** non-regulated customer accounts in **15** states



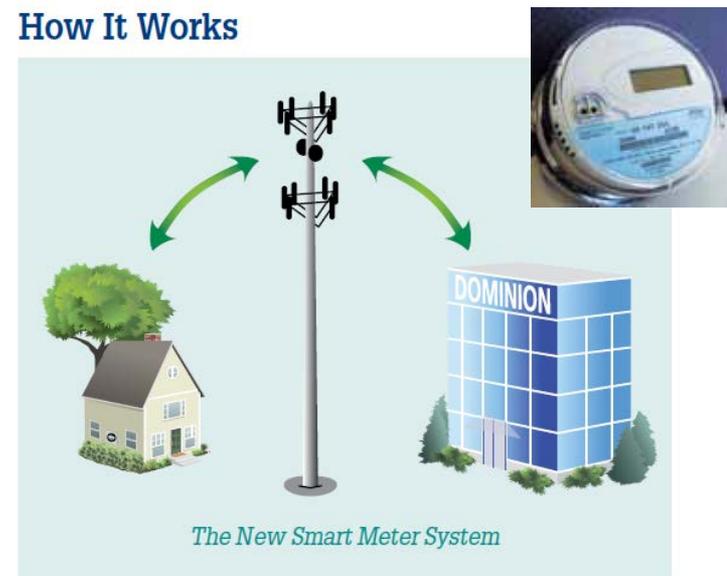
Electric Distribution

Smart Meter Technology Program

- More than **100,000** smart meters have been successfully deployed in 3 geographic areas in Virginia since 2009
- Part of a multi-phased evaluation and ongoing testing to confirm anticipated results for customers
- Plan to install **~8,000** meters to evaluate additional technology by end of 2011 in Blue Ridge, downtown Richmond, and Williamsburg, Virginia
- Capabilities and benefits
 - Remote meter reading
 - Voltage conservation
 - Outage and restoration notification
 - Remote meter connect/disconnect
 - Dynamic pricing



How It Works

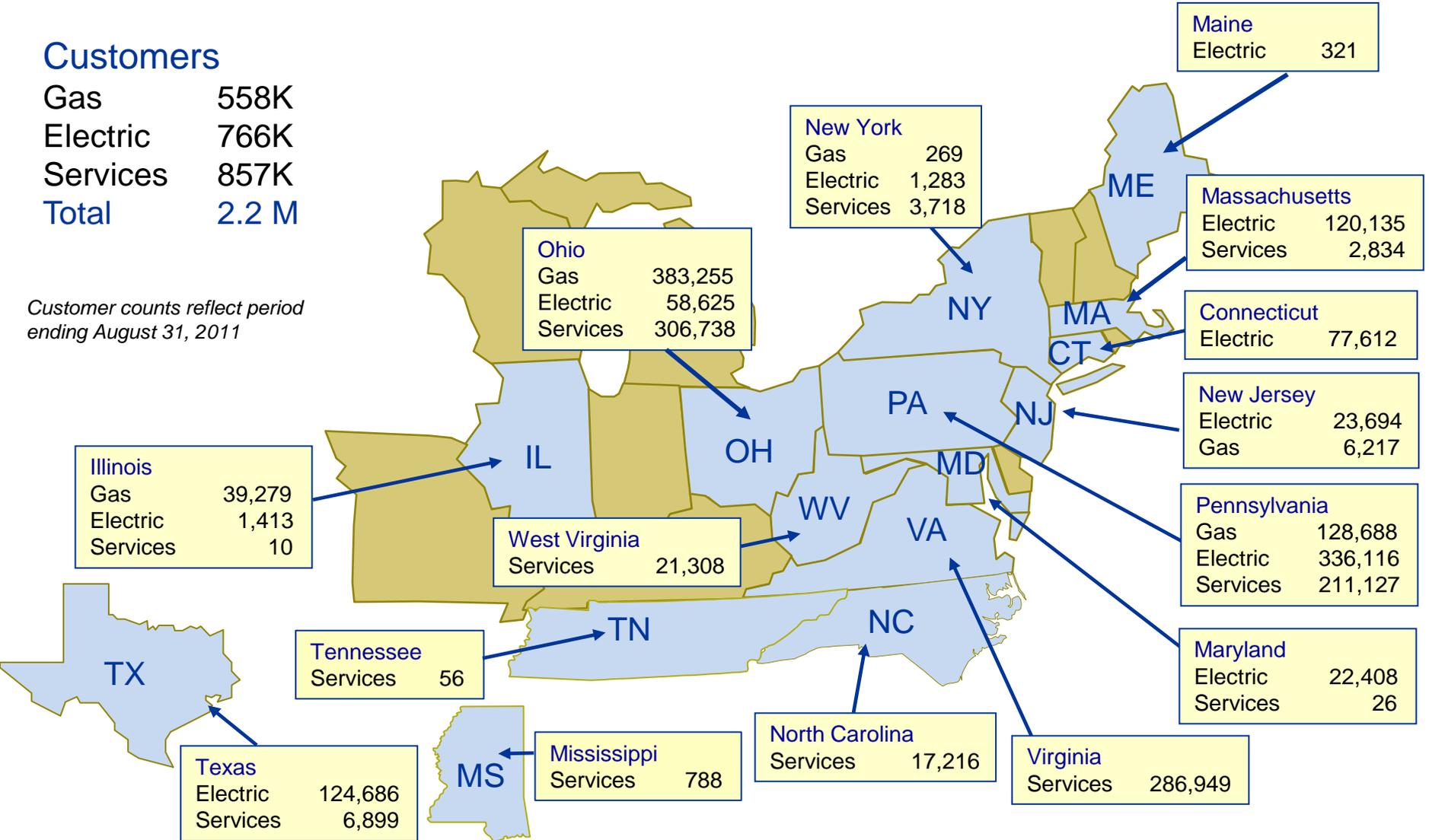


Dominion Retail Markets

Customers

Gas 558K
 Electric 766K
 Services 857K
 Total 2.2 M

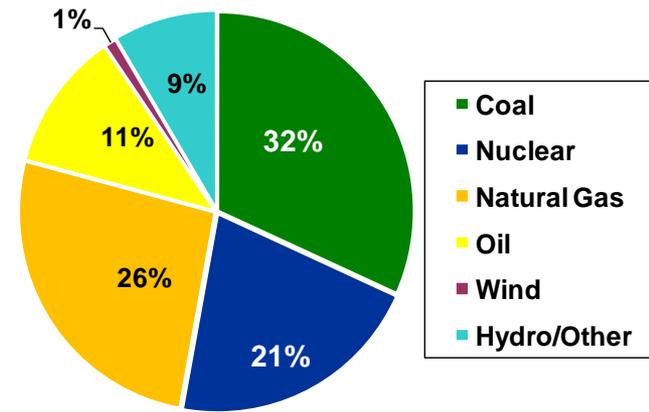
Customer counts reflect period ending August 31, 2011



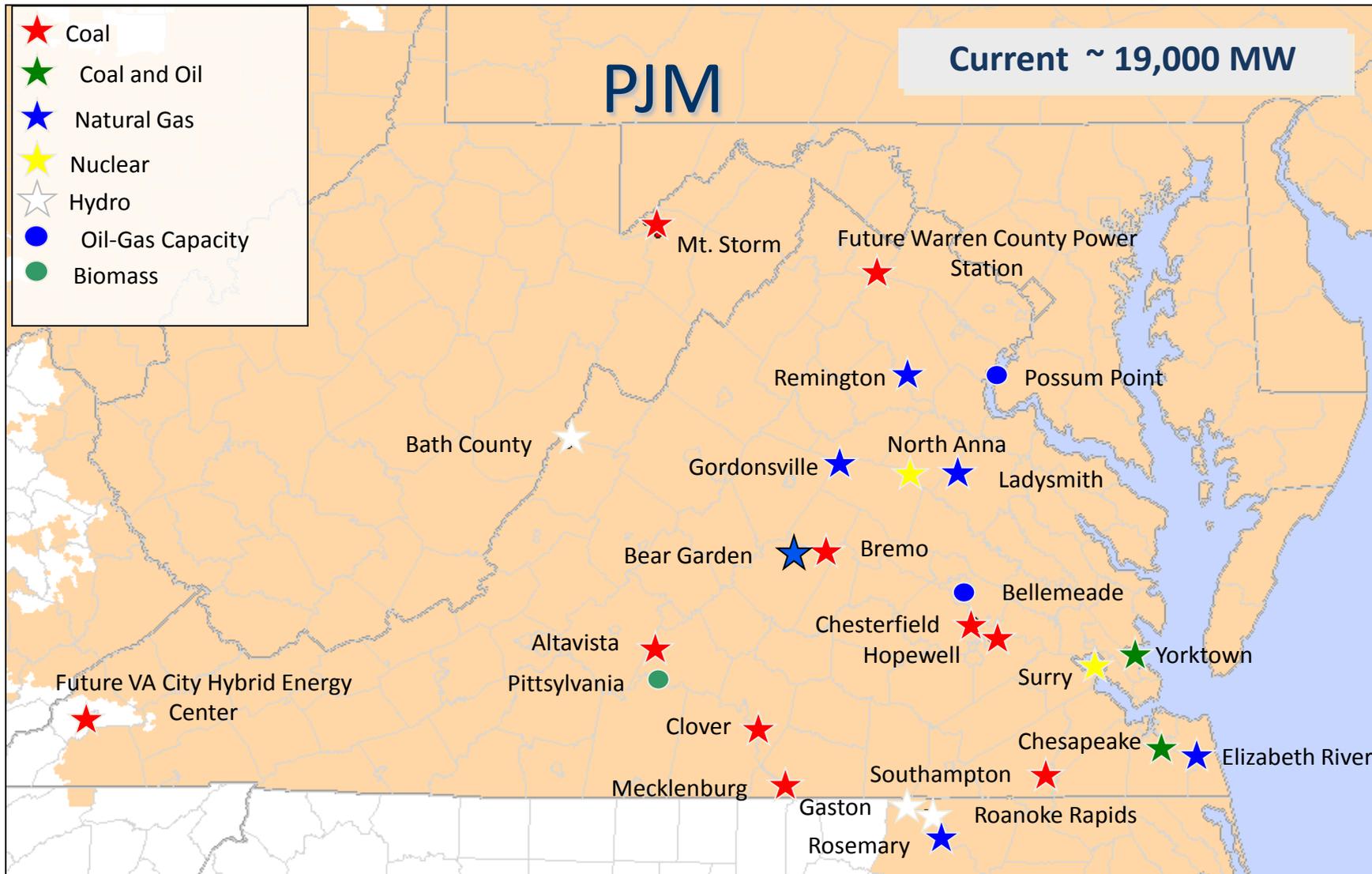
Dominion Generation Profile

- Approximately **28,000** megawatts of generating assets
 - ~**19,000** megawatts regulated utility
 - ~**9,000** megawatts merchant
 - Balanced, diverse fuel mix
- Utility Generation
 - Division of VEPCO
 - Additional **4,550 MW** needed during next decade to meet load growth
 - Rider projects to support growth underway
 - Virginia fuel factor reset effective July 1st of each year
- Merchant Generation
 - Well-positioned in New England and PJM power markets
 - **More than 80%** of production from baseload coal and nuclear
 - Active hedging program for energy revenue/margins

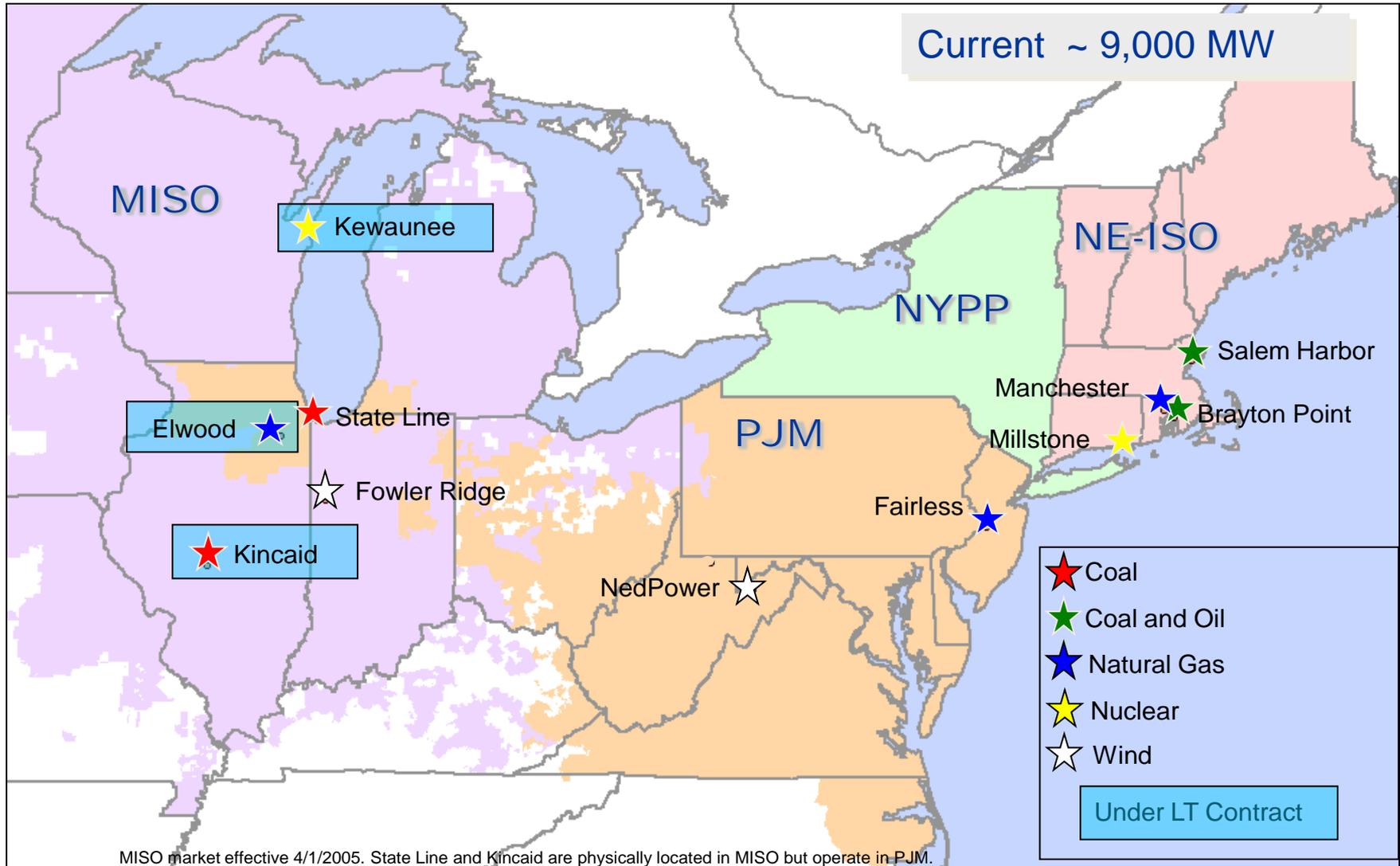
2010 Electric Capacity by Fuel
Total Fleet



Utility Generation Portfolio



Merchant Generation Portfolio



Dominion Energy Profile

☐ Gas Transmission

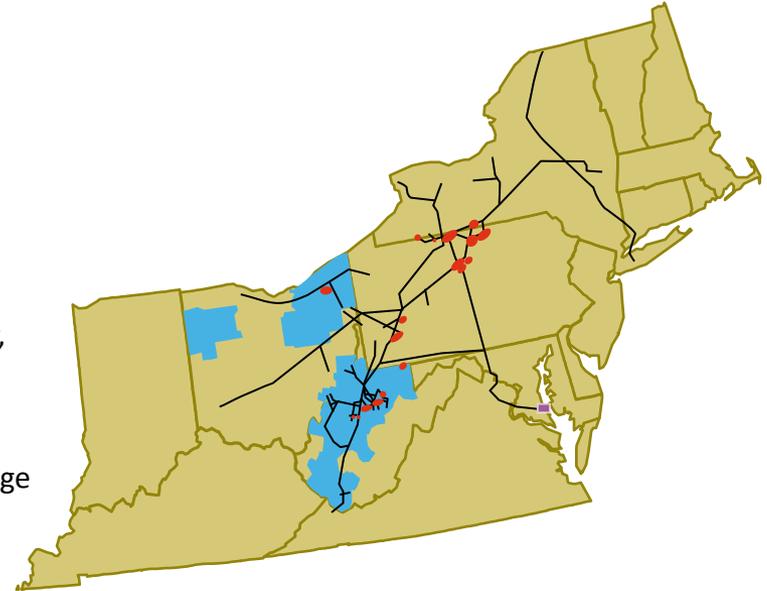
- Dominion Transmission
 - 7,979 miles of pipeline in six states
 - 776 Bcf of underground natural gas storage
 - 7.2 Bcf/d gas peak sendout capability
 - 278 MMcf/d of natural gas processing capacity*
 - Estimated NGL sales of ~160-165 million gallons per year, plus 8-12 million gallons of fee-based NGL
- Dominion Cove Point LNG
 - 1.8 MMDth/d of LNG send-out with 14.6 Bcf of LNG storage

☐ Gas Distribution

- Dominion East Ohio and Dominion Hope
 - 171 Bcf of underground natural gas storage
 - 1.3 million natural gas customers
 - 272 Bcf of natural gas throughput in 2010
 - 21,800 miles of natural gas distribution pipeline

☐ Producer Services

- Unregulated gas operations



— 11,000 miles of natural gas transmission, gathering and storage pipeline

● 947 billion cubic feet of natural gas storage operated

■ Cove Point LNG Facility

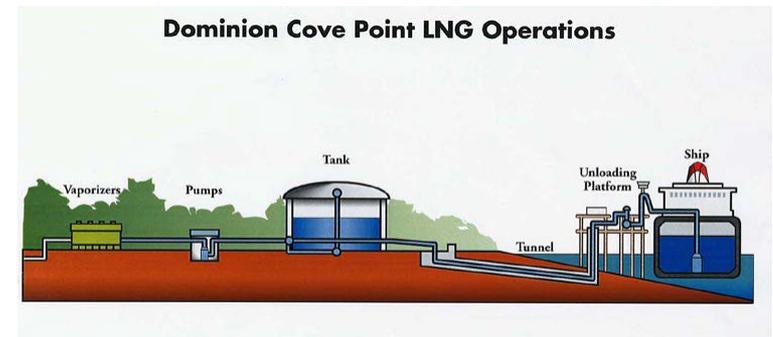
■ 1.3 million natural gas customers in OH & WV

* Does not include the Natrium facility which is under construction

Gas Transmission

Cove Point LNG Facility*

- ❑ Exploring liquefaction possibilities
- ❑ Ideally sited in the Mid-Atlantic to capitalize on Marcellus and Utica shale production
- ❑ Dominion's interest would be limited to the facility, not the commodity
- ❑ First Steps:
 - File application with DOE for LNG export authorization to
 - Free Trade Agreement countries (approved 10/7)
 - Non-Free Trade Agreement countries (filed 10/3)
 - Pre-file with FERC for additional authorization for LNG exportation

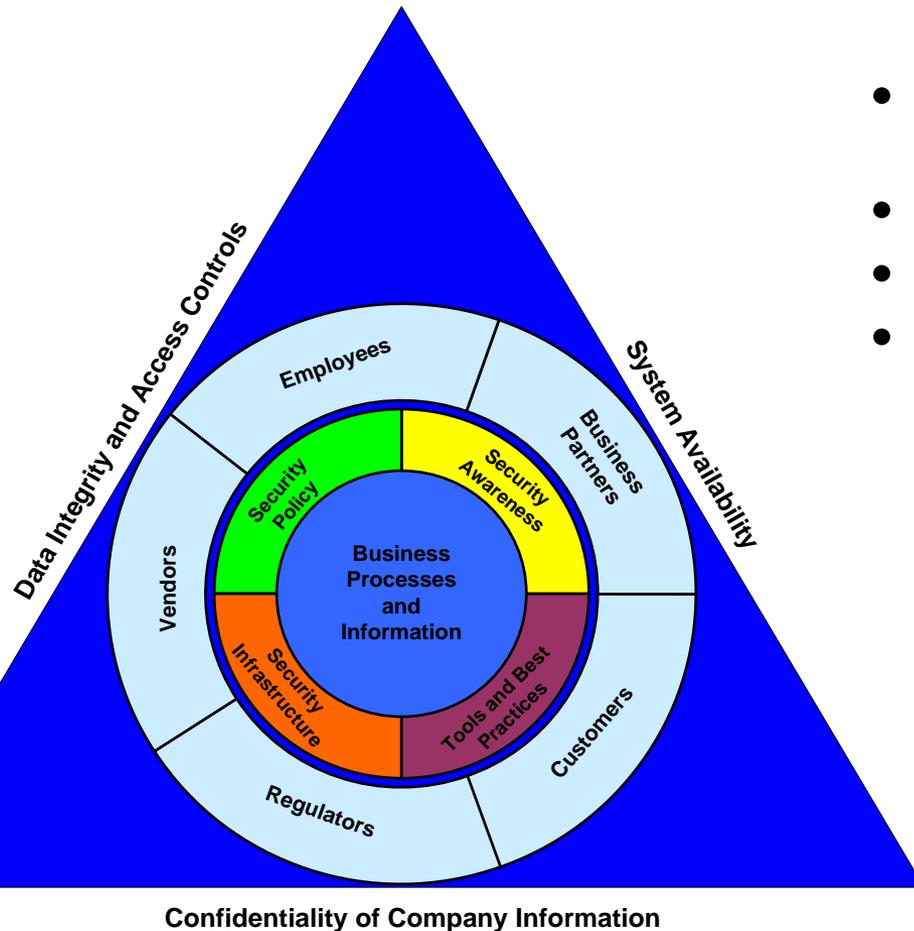


*Not included in Planned or Potential Growth Capex

Discussion Topics

- Brief Overview of Dominion
- **Dominion's Cyber Security Program**
- The Current Landscape
- Threats and Vulnerabilities
- Regulatory and Legislative Update

Dominion - Cyber Security Framework

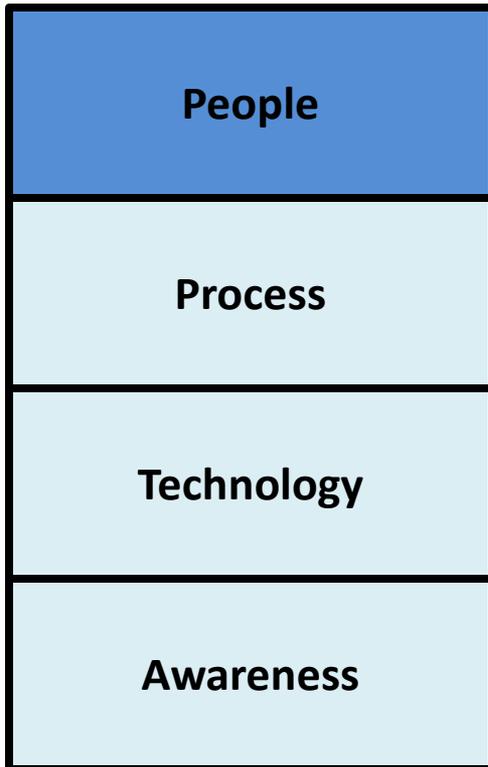


- Sensitive and Confidential Information
- Financial Systems
- Business Network
- Critical Infrastructure
 - Electric SCADA and Transmission Substations
 - System Operations Centers
 - Gas SCADA and compressor stations
 - Cove Point
 - Nuclear and F&H Process Control Systems

Cyber Security Program

Continuous Monitoring and Oversight

☐ People



- IT Risk Management
 - Policy and Compliance
 - Security Architecture
 - Risk Management Strategic Initiatives
 - Business Resumption Planning
 - Records and Litigation Management
 - Self Assessment Program
 - Liaison with Auditing, Law, Regulators, HR
- Business Area Risk Managers (Application Security)
- Risk Operations
 - Firewall Administrators
 - Mainframe Security
 - Enterprise User Security Administration
 - Workstation and Server Administrators
 - Email/SPAM Security
 - Cyber Security Operations Center (CSOC)

Information Sharing

❑ Industry Organizations

- Edison Electric Institute Security Working Group
- American Gas Association (AGA) Security Working Group
- Interstate Natural Gas Association (INGAA) Control Systems Cyber Security Working Group
- North American Electricity Reliability Corp (NERC) Critical Infrastructure Protection Committee
- NERC Control System Security Working Group (CSSWG)
- DHS Industrial Control System Joint Working Group (ICSJWG)
- Southeastern Electric Reliability Corp (SERC) Critical Infrastructure Protection Committee
- SERC Cyber Security Compliance Advisory Group (CSCAG)
- Reliability First Corp (RFC) Critical Infrastructure Protection Committee
- Northeast Power Coordinating Council (NPCC) Task Force for Information Security
- Nuclear Information Technology Strategic Leadership (NITSL)
- Nuclear Energy Institute (NEI) Cyber Security Task Force
- DHS Cross Sector Security Working Group (CSCSWG)
- Infraguard (FBI)
- National Institute of Standards and Technology (NIST) Smart Grid Interoperability Panel
- Utility Communications Architecture International Users Group (UCAIug)
- North American Transmission Forum
- Midwest Reliability Organization (MRO) Critical Infrastructure Protection Committee
- National Electric Sector Cybersecurity Organization (NESCO)

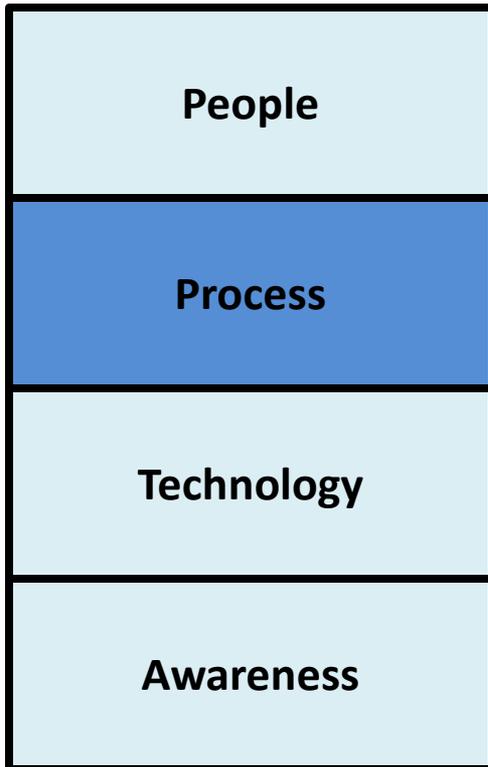
❑ Classified Threat Information from:

- DHS, DOE, DOD, National Labs, FBI, NRC

Cyber Security Program

Continuous Monitoring and Oversight

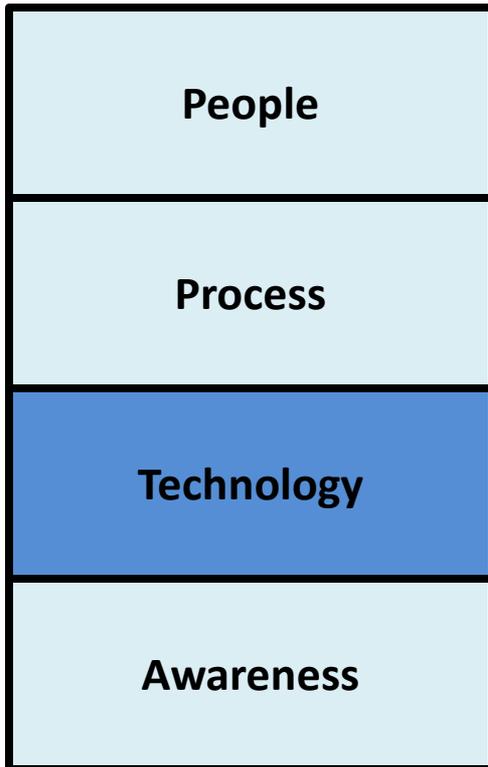
❑ Process



- Security Policy Compliance and Enforcement
- Random Sweeps of Critical Devices
- Internal and External Auditing of Controls
- Reviews of Controls by Peer Companies
- Business Resumption and Technical Recovery
- Incident Response Team and Testing
- Vulnerability Management
 - Identify and rate vulnerabilities
 - Use third-party to test defenses at key points inside and outside the network
 - o Dominion’s Internet Connections
 - o Electric Transmission network
 - o Gas Transmission network
 - o Generation process control networks (Nuclear and F&H)
 - o Wireless network

Cyber Security Program

Continuous Monitoring and Oversight

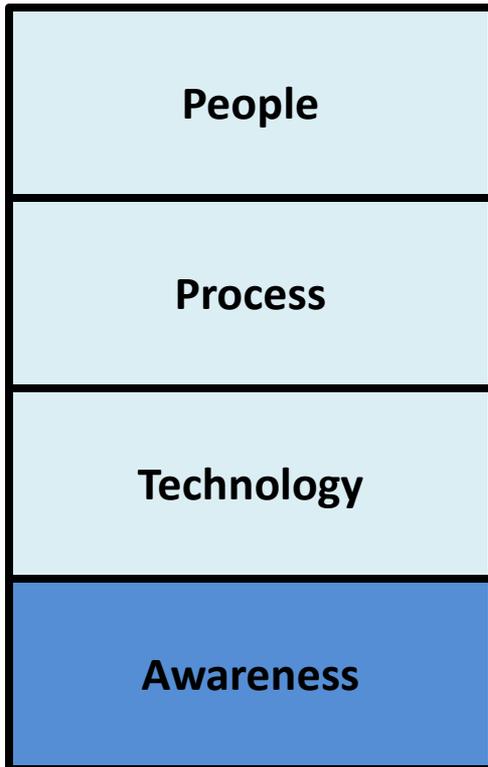


☐ Technology

- Access Controls
- Encryption
- Wireless Security and Rogue Access Point Detection
- Laptop Hard Disk Encryption
- Firewalls
- Intrusion Detection and Prevention
- Internet Content Filtering
- Virus and Malware protection
- Security Patch Management
- Application Security
- Secure E-mail
- Security Event Information Manager

Cyber Security Program

Continuous Monitoring and Oversight



Security Awareness

- Online Training
- Logon Banners
- Connect Today Articles
- Management Training
- Management Newsletters
- Pop-up Screens
- Technical Newsletters
- Videos
- E-mails
- Posters
- Brochures
- Face to Face at Company Meetings

Discussion Topics

- Brief Overview of Dominion
- Dominion's Cyber Security Program
- **The Current Landscape**
- Threats and Vulnerabilities
- Regulatory and Legislative Update

Cyber Security Reality



***Debora Plunkett, head of the
NSA's Information Assurance
Directorate – December 2010***

No computer network can be considered completely and utterly impenetrable - not even that of the NSA

Attackers, backed by governments and intelligence organizations, are usually highly motivated and often very well funded.

Attackers have time, money and incentive to keep at it as long as it takes to identify that crack in the armor that will allow them to get in.

... the main aspect of cyber defense that every one should concentrate on is real-time detection of intrusions that would allow defenders to actively fight off the attackers

Public Media Attention

FINANCIAL TIMES

October 11, 2011 5:26 pm

US power plants vulnerable to cyberattack



Night Dragon Cyber Attacks Hit Oil Firms

TECHNOLOGY - SCITECH

Stuxnet Clone 'Duqu' Possibly Preparing Power Plant Attacks

By Matt Liebowitz

Published October 18, 2011 | TechMediaNetwork

NSA Chief Questions E-Grid Safety

Industry's Ability to Protect Power Grid in Doubt, Alexander Says

Zero-day flaws found in SCADA systems

By Jaiukumar Vijayan

October 10, 2011 08:00 AM ET

 Add a comment  Like  Confirm  +1  2

Computerworld - An Italian security researcher recently disclosed details about several zero-day vulnerabilities in supervisory control and data acquisition (SCADA) systems from several vendors.



Public Media Attention

Opinion: Computer worm could multiply San Bruno type disasters – San Jose Mercury News

webmaster@technorati.com wrote an interesting post today on Here's a quick excerpt

Opinion: Computer worm could multiply San Bruno type disastersSan Jose Mercury NewsMeanwhile, halfway around the world, a newly discovered self-propagating computer worm has been silently infecting tens of thousands of industrial systems ...and more »

San Diego blackout highlights infrastructure vulnerabilities

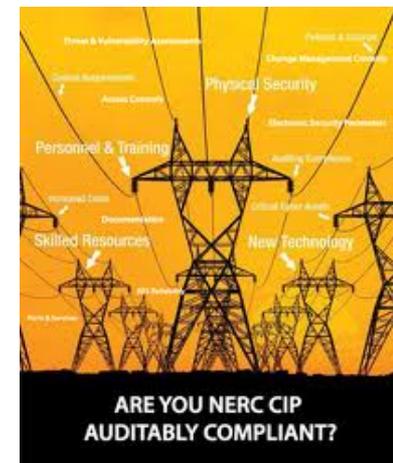
10 years after 9/11, cyberattacks pose national threat, committee says

Catastrophic cyberattacks are not 'science fiction,' says the Bipartisan Policy Center

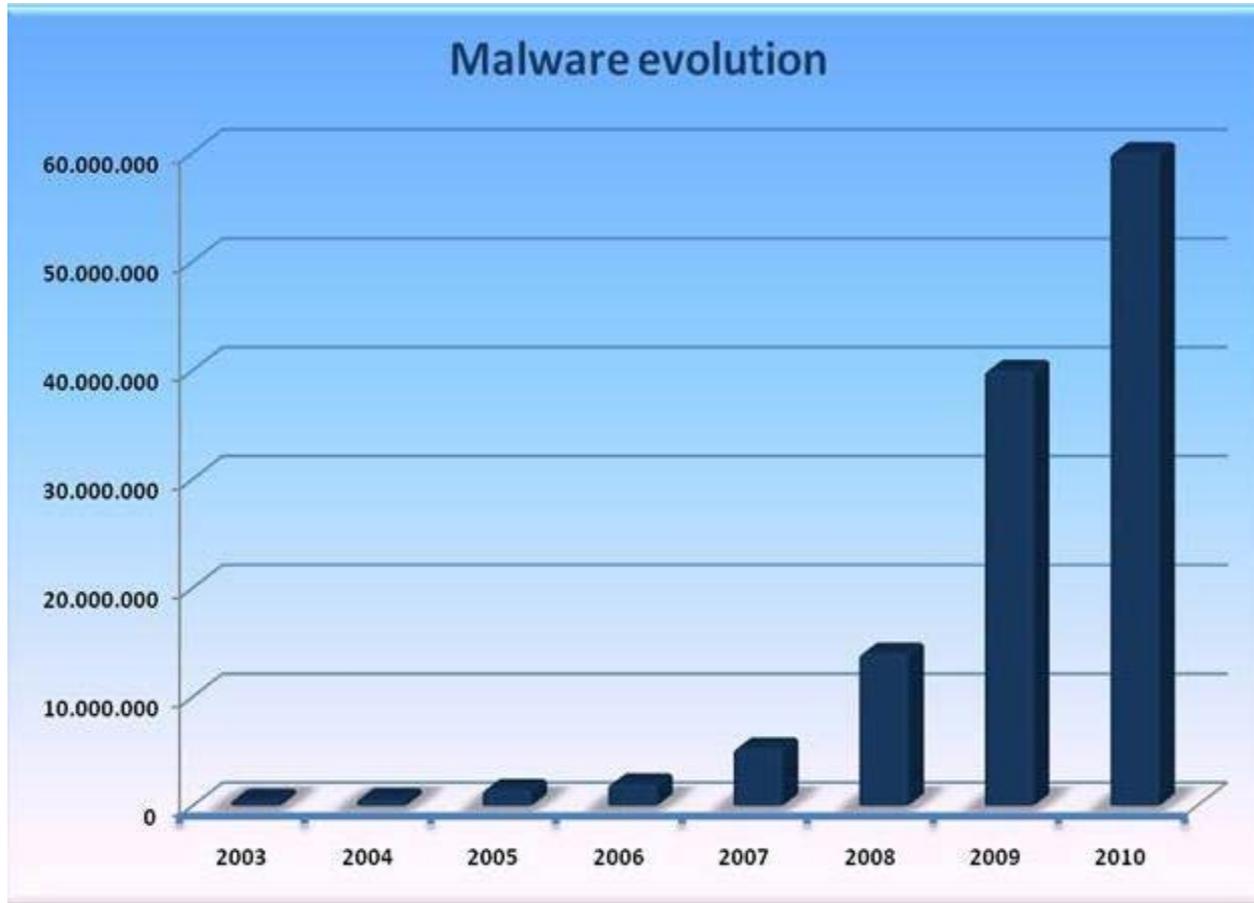
Smart grid cybersecurity standards still lacking, says GAO

Homeland Security must address 'weaknesses,' GAO says

The GAO Report Nudges NIST and FERC on Cybersecurity



Exponential Growth



One third of all malware was created in the first 10 months of 2010.

The average number of malware threats **created every day**, including new malware and variants of existing families, has risen from 55,000 in 2009 to 63,000 in 2010 – a rate increase of 14.5 percent.

The average lifespan of 54 percent of malware has been **reduced to just 24 hours**, compared to a lifespan of several months that was more common in previous years.

Our Operating Environment

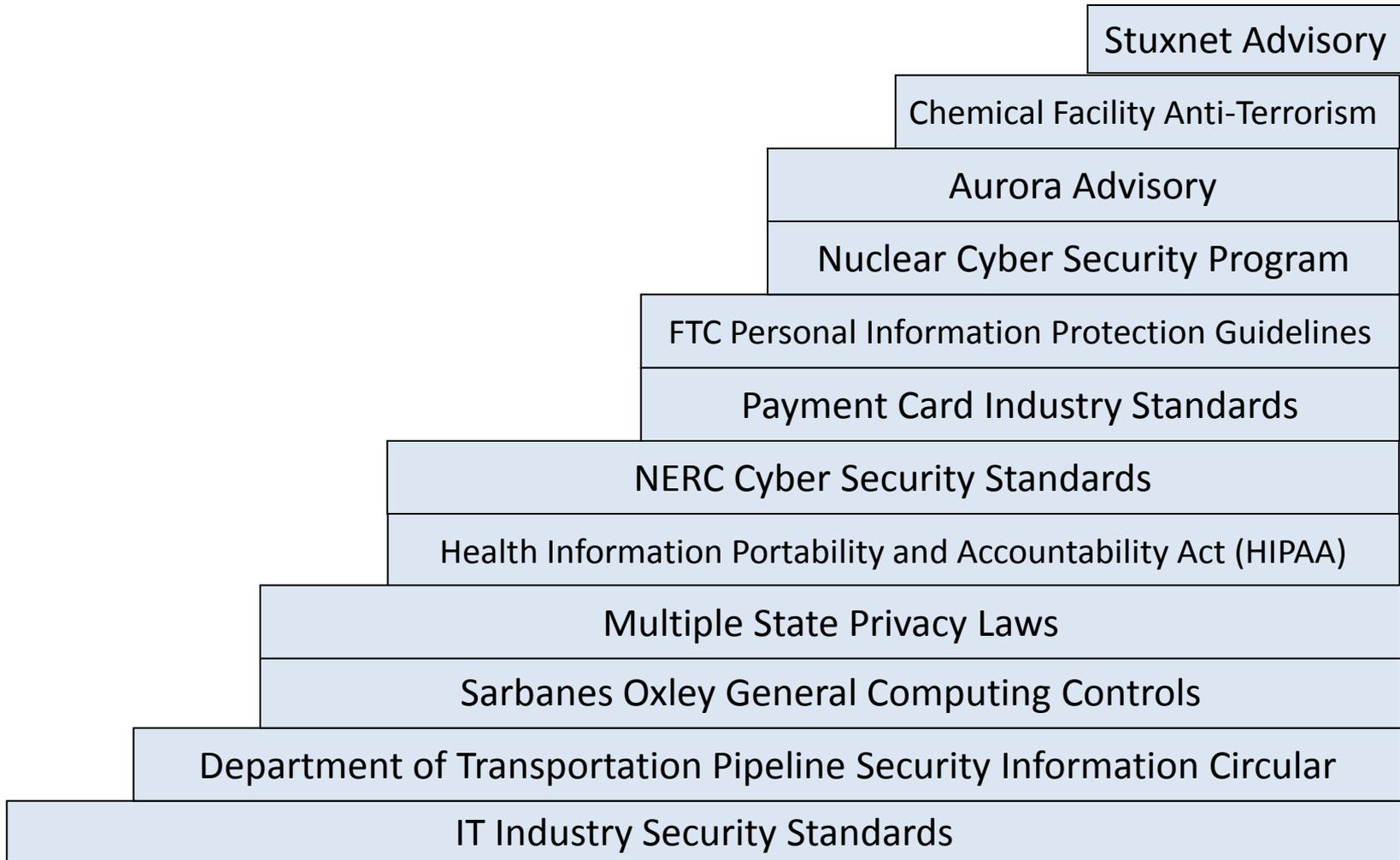


Energy Cyber Security is Different: IT vs. ICS Security

Topic	Information Technology	Industrial Control Systems
Anti-Virus/Mobile Code	Common, widely used	Uncommon, impossible
Typical Lifespan	3-5 years	15-20 years
Outsourcing	Common, Widely used	Rare, uncommon
Patch Management	Regular, scheduled	Slow, vendor-specific
Change Management	Regular, scheduled	Uncommon
Time Critical Content	Generally delays accepted	Critical due to safety
Availability	Generally delays accepted	24 x 7 x 365 x forever
Security Awareness	Good	Poor, except physical
Security Testing/Audit	Scheduled, mandated	Occasional , uncommon
Physical Security	Secure	Remote and unmanned

Source: Department of Energy

Compliance Pyramid

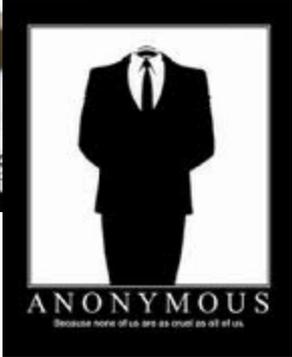
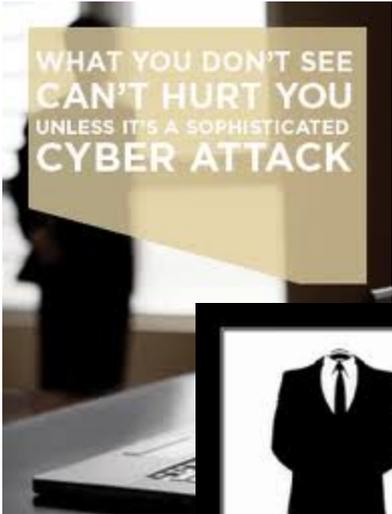


Pre 2002	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
----------	------	------	------	------	------	------	------	------	------	------

Discussion Topics

- Brief Overview of Dominion
- Dominion's Cyber Security Program
- The Current Landscape
- **Threats and Vulnerabilities**
- Regulatory and Legislative Update

Threats



Cyber Threat Groups

- Nation States
- Terrorists
- Criminals
- Hacktivists
- Hackers
- Insiders

Country/Region	% Traffic	Q1 '10 %
1 United States	11%	10%
2 China	11%	9.1%
3 Russia	10%	12.0%
4 Taiwan	6.0%	6.1%
5 Brazil	6.0%	6.0%
6 Italy	3.0%	4.4%
7 Germany	3.0%	3.9%
8 Romania	2.0%	2.2%

Figure



Threats

Cyber Threat Group	Primary Motivation	What they want	How they get it
Foreign State	National interests	Information	CNE
	Warfare	Control	CNA
Terrorist	Ideology	Attention	CNA
Criminal	Money	PII	CNE
		Ransom	CNA
Hacker	Personal Interest	Methods	CNE
Hacktivist	Cause	Support	CNA
Insider	Anger	Revenge	CNA
	Personal Enrichment	Information	CNE

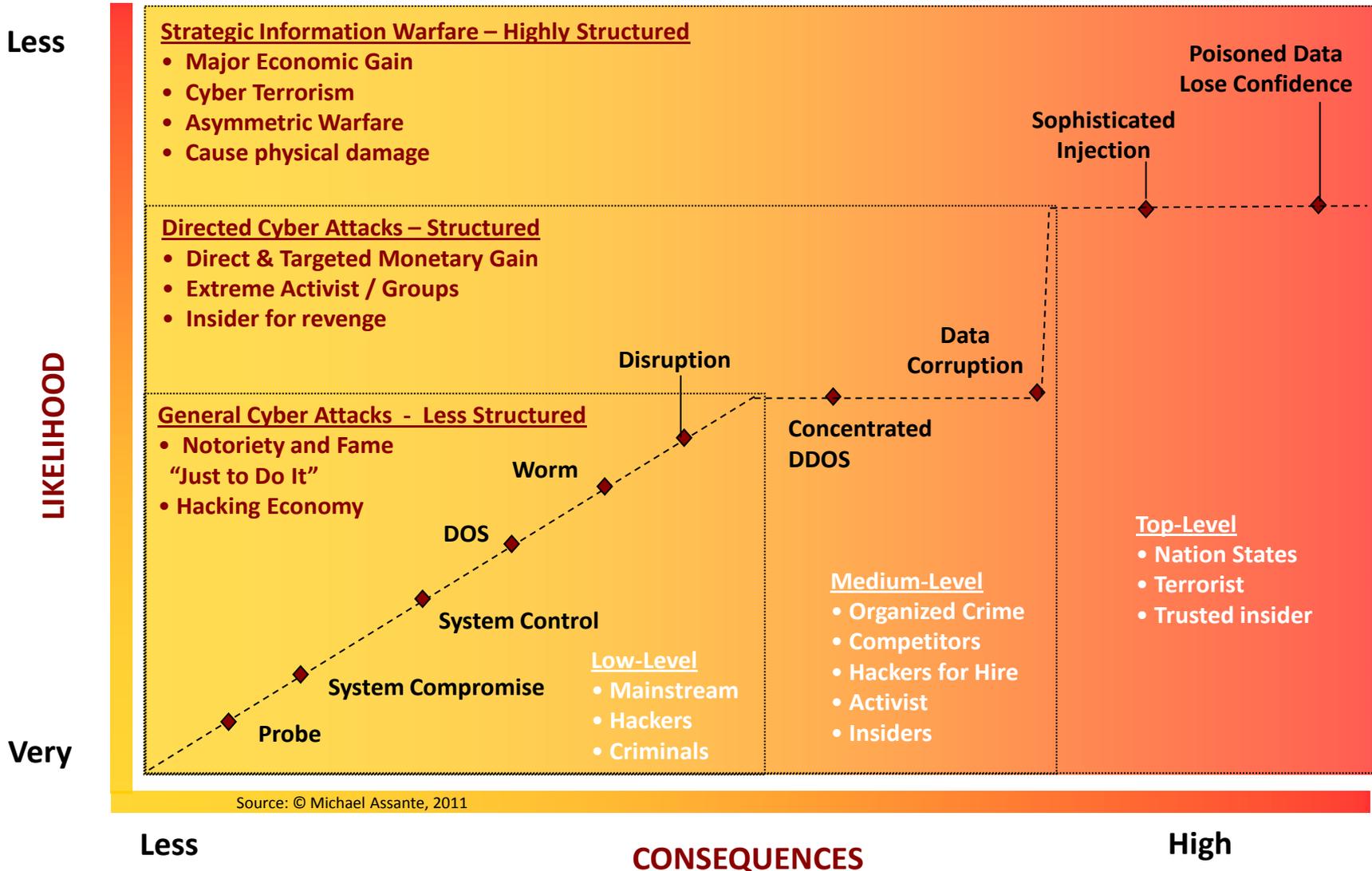


CNE – Cyber Network Exploitation (non-destructive)

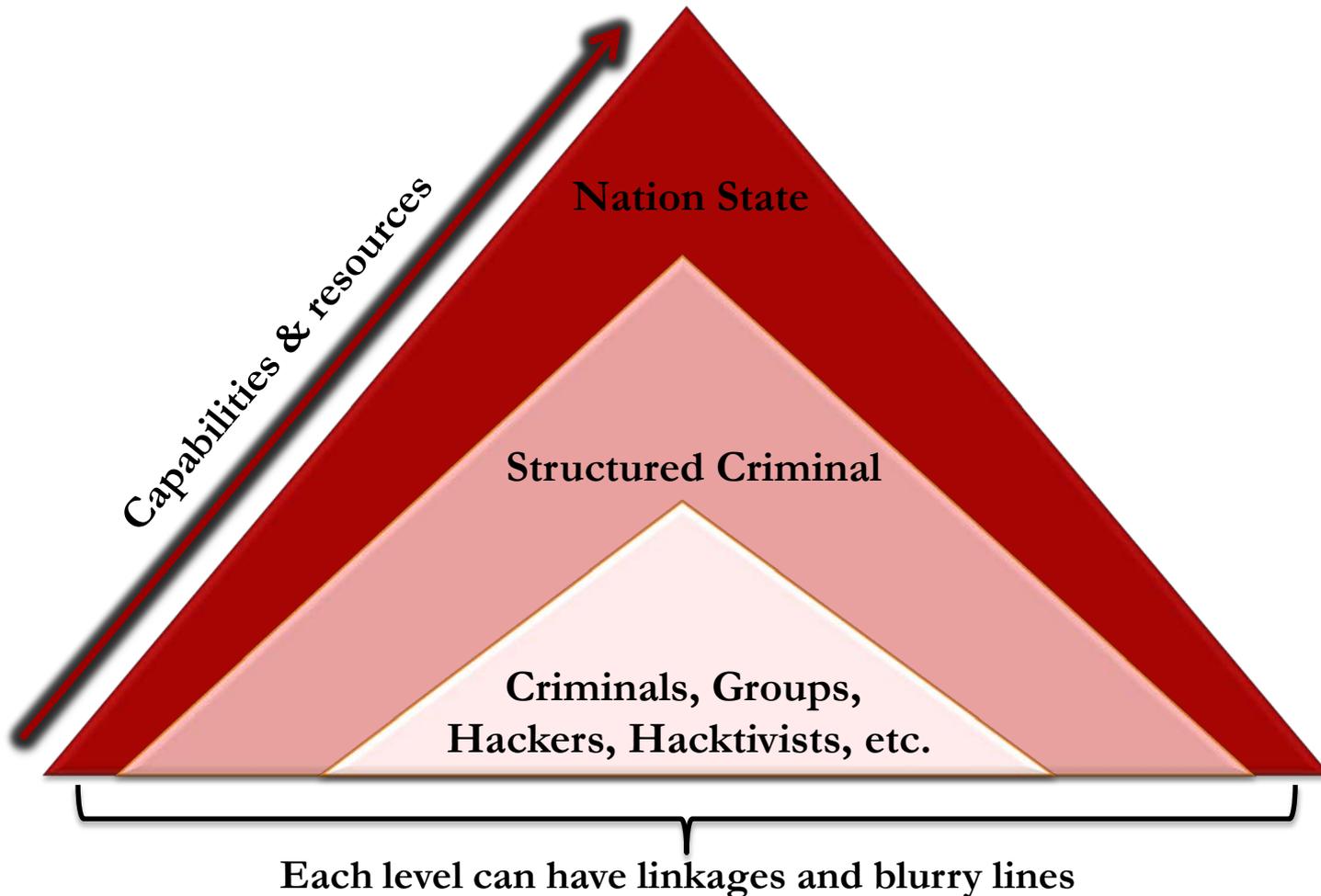
CNA – Cyber Network Attack (Destructive)

FBI – US Electricity Sector Faces High Cyber Exploitation Threat, Low Cyber Attack Threat

Potential Adversaries



Adversary Capabilities



Adversary Capabilities

Low Level Threat

Criminals, Hackers, Hacktivists

- Can be less experienced
- Limited financial resources
- Opportunistic in nature
- Target known vulnerabilities
- Use packaged attack tools
- Can be motivated by bragging rights, theft, activism, exploration
- Market provided defenses are usually effective

Medium Level Threat

Structured Criminal

- Can be experienced and skilled
- Access to financial resources
- Targeted in their attacks
- Posses objectives
- Use a range of attack tools
- Can be detected
- Exploit known vulnerabilities very quickly

High Level Threat

Nation State

- Draw upon skilled people
- Demonstrate sophisticated tactics
- Deep financial resources
- Rely on recon and planning
- Target specific technologies & data
- Develop customized attacked tools
- Can exploit unknown vulnerabilities
- Well defined goals & objectives
Difficult to detect & remove
- Can use insider access
- Access to supply chains

Adversary Capabilities

High Level Threat Actors have the capability to employ or exploit all of the following:

Network traffic capture and analysis

Intercept and modify data inputs and outputs

Inject values or data into bidirectional traffic (Man-In-The-Middle attacks)

Physical layer (tampering, inputs and add-ons)

Data & datalink layer (MAC address spoofing, root bridge, enable unauthorized DHCP server, VLAN trunking, etc.)

Network layer (injecting blackhole, rerouting, rout manipulation, inject packets and malformed packets, source route IP packets, etc.)

Application layer (DNS cache poisoning, web browser attacks, digital certificate impersonation, TCP session hijacks, injects)

System layer (OS attacks, privilege escalation, remote control, computer resource management, etc.)

Behavioral (people) layer (man-to-machine interface and process)

Compromising and owning a connected device with administrative privileges

Denial of Service attacks (Complete, Selective, etc.)

Weak authentication/authorization

Buffer Overflows

Integer Over/Underruns

Format String Flaws

Use of fuzzers and other logic flaws

Consider OS and application flaws (evaluate common code weaknesses/programming errors and IT vulnerabilities)

Connected devices, servers, and databases (injection attacks)

Access to computer resource management (the actual board)

Process for updates (Supply Chain, vendor patch management)

Anonymous and Lulzsec

UNCLASSIFIED



NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0010-NCCIC -160020110719

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

"ANONYMOUS" AND ASSOCIATED HACKER GROUPS CONTINUE TO BE SUCCESSFUL USING RUDIMENTARY EXPLOITS TO ATTACK PUBLIC AND PRIVATE ORGANIZATIONS

Organizations attacked by Anonymous or Lulzsec:

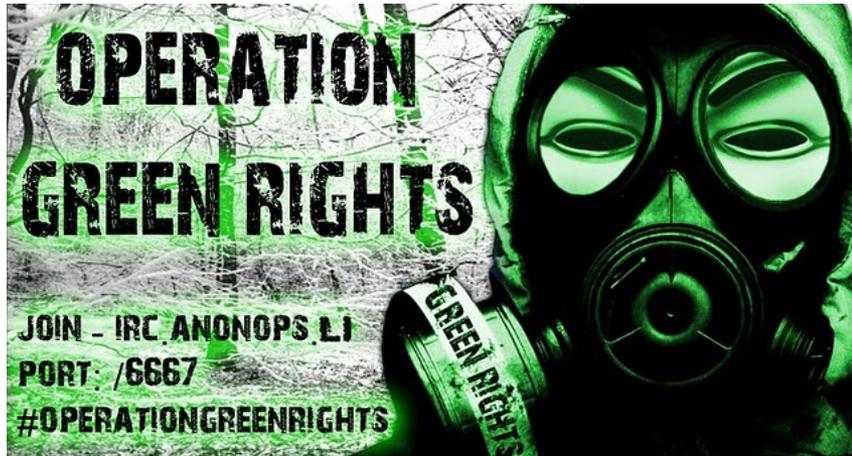
- Sony
- Amazon
- Bay Area Rapid Transit (San Francisco)
- HB Gary (Security Firm)
- Master Card
- Paypal
- Motion Picture Association of America
- Record Industry Association of America
- Bayer
- Monsanto
- FBI - Infraguard
- CIA
- US Senate
- Nintendo
- Fox News
- PBS
- Booz Allen Hamilton
- Viacom
- Universal Music
- Vanguard Defense Industries
- Mantech (Defense Contractor)
- Arizona Department of Public Safety
- CBS



A N O N Y M O U S



Anonymous



Operation Green Rights - foreign energy companies targeted – GE, EDF and Eon

Anonymous hackers Starts Project Tarmeggedon , Presents by Operation Green Rights. Hackers calling everyone to Protest.

Press Release By Anonymous Hackers :

Free-thinking citizens of the world:

Anonymous' Operation Green Rights calls your attention to an rgent situation in North America perpetuated by the boundless greed of the usual suspects: Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, the Royal Bank of Scotland, and many others.

This week, activists are gathering along U.S. Highway 12 in Montana to protest the transformation of a serene wilderness into an industrial shipping route, bringing "megaloads" of refinery equipment to the Alberta Tar Sands in Canada (see Tar Sands FAQ Sheet below).

Anonymous now joins the struggle against "Big Oil" in the heartland of the US. We stand in solidarity with any citizen willing to protest corporate abuse. Anonymous will not stand by idly and let these environmental atrocities continue. This is not the clean energy of the future that we are being promised

Project Tarmeggedon by Anonymous Hackers **Operation Green Rights**

Anonymous

DHS: Anonymous Interested in Hacking Nation's Infrastructure

UNCLASSIFIED//FOR OFFICIAL USE ONLY



NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0020-NCCIC / ICS-CERT -120020110916



DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR MISSION PARTNERS AT THE "FOR OFFICIAL USE ONLY" LEVEL, ACROSS THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

(U//FOUO) ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS

(U) On 19 July 2011, a known Anonymous member posted to Twitter the results of browsing the directory tree for Siemens SIMATIC software. This is an indication in a shift toward interest in control systems by the hacktivist group.

<http://www.wired.com/threatlevel/2011/10/hacking-industrial-systems/>

DHS Note on Insider Threat to Utilities

UNCLASSIFIED//FOR OFFICIAL USE ONLY



(U//FOUO) Insider Threat to Utilities

19 July 2011

(U) Prepared by the Office of Intelligence and Analysis (I&A), Cyber, Infrastructure, and Science Division, Strategic Infrastructure Threat Branch and Cyber Threat Analysis Branch. Coordinated with the Control Systems Security Program, Industrial Control Systems-Computer Emergency Response Team; Environmental Protection Agency; and the Department of Energy.

During Classified Briefing on July 23rd, DHS confirmed there was no specific threat that caused the release of this Note.

NERC, NRC, NEI and several utilities provided comments to media requests.

July 21st - Terrorists looking to attack U.S. utility facilities, report warns - A new intelligence report warns that extremists are looking to attack a U.S. utility company and have in fact attained insider positions and tried to coax information from utility-sector employees, [ABC World News reports](#).

"Based on the reliable reporting of previous incidents, we have high confidence in our judgment that insiders and their actions pose a significant threat to the infrastructure and information systems of U.S. facilities," the bulletin from the Department of Homeland Security reads in part, [World News quotes](#). An attack on a utility company could cause potentially cause significant damage and casualties.

July 22nd - US utilities say ready for any potential threats to infrastructure - The US electric reliability watchdog and the power sector said Thursday that they are working with federal authorities and within the industry to shore up security in the face of a recent federal bulletin about potential threats to private sector utilities. The Department of Homeland Security issued the bulletin on Tuesday.

Spear Phishing Attacks Against Utilities

OFFICIAL USE ONLY - SECURITY-RELATED INFORMATION



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

July 28, 2011

INFORMATION ASSESSMENT TEAM ADVISORY FOR SELECTED POWER REACTORS, NON-POWER REACTORS, DECOMMISSIONED REACTORS, CATEGORY I AND III FUEL FACILITIES, GASEOUS DIFFUSION PLANTS, INDEPENDENT SPENT FUEL STORAGE FACILITIES, CONVERSION FACILITY AND FOR LARGE MATERIALS LICENSEES (NRC AND AGREEMENT STATES) WHO POSSESS, SHIP OR RECEIVE CERTAIN QUANTITIES OF RADIOACTIVE MATERIALS

IA-11-03

SUBJECT: SPEAR PHISHING ACTIVITY RELATED TO NMMSS NEWSLETTER

July 25 - attackers with characteristics known to be associated with China sent a targeted spear-phishing e-mail containing a malicious payload to multiple employees using a publicly available e-mail list for DOE's Nuclear Material Management and Safeguards System (NMMSS).

The incident was subsequently reported to U.S. CERT and shared with members of the UNITE Security Directors Council, as well as trusted industry peers at NERC, DOE and NEI.

UNCLASSIFIED // FOR OFFICIAL USE ONLY



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-231-01P—CRITICAL INFRASTRUCTURE SPEAR PHISHING CAMPAIGN

August 19, 2011

ALERT

July 26 - the NRC (Nuclear Security and Incident Response Branch) issued an advisory on this topic on their protected website.

Threats - Aurora

Recommendation to Industry
AURORA Mitigation - Protection and Control Engineering Practices and Electronic and Physical Security Mitigation Measures

[Acknowledge](#) [Add](#)

Distribution Date: October 13, 2010 10:15 AM CST

Status: Acknowledgment Required by *October 18, 2010*
Response Required by *December 13, 2010*

 **Sensitive:** Internal Use Only (Do Not Distribute Outside Your Company)

Instructions: This NERC Recommendation is not the same as a Reliability Standard, and for an enforcement action. However, pursuant to Rule 810 of NERC's Rule Recommendation and report to NERC on the status of your activities in relation to the Aurora threat and report them to the Federal Energy Regulatory Commission (FERC) for its purposes but will not include those responses in the compilation it sends to the public.



- Original Alert issued by NERC and NRC in 2007
- Initial protections implemented in all Business Areas
- Expanded scope of vulnerability identified in 2010

What is Aurora

❑ Rotating equipment such as motors and generators spin in sync with the power grid.

- Rotating equipment brought onto or reconnected to the grid out of sync, or “out of phase,” can lead to damaging torques as the machine is forced back into synchronization
- Resulting torque can exceed mechanical design limits, damaging or destroying rotating equipment and connected loads, i.e., pumps and gear boxes.
- Historical incidents of accidental malfunction and mis-operation show that risk of damage from inadvertent reclosures is real and persistent.

❑ AURORA describes a narrow, but significant gap in contemporary protection that allows out-of-synch events to occur.

- AURORA can occur accidentally or intentionally.
- AURORA “attack” is simply a deliberate attempt to damage or destroy susceptible equipment.
- Facilities that implement all traditional physical and cyber security best practices may still be vulnerable to an AURORA initiated from outside their fence. One need only gain physical or cyber access to a relevant upstream commercial substation breaker.

❑ An assessment can help determine susceptibility and facilitate mitigation



In-Phase



Out-of-Phase

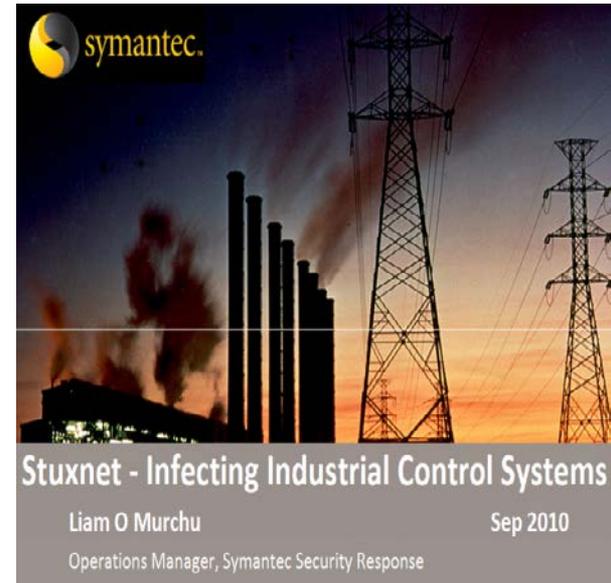
Threats - Stuxnet

Recommendation to Industry Exploit Active for - Malware Targeting SCADA Systems (Update 3)

Distribution Date: September 13, 2010 5:15
PM CST
Initial Distribution: July 20, 2010 (As Advisory)
Additional Information Distributed: August 3,
2010 (As Advisory)

**Active Stuxnet exploits overseas in
Industrial Control Systems
necessitate new recommendations
from NERC CIP Malware Tiger Team,
Microsoft, Siemens, and ICS-CERT.**

Please note that Acknowledgement and
Response Due Dates are based on 20:00
Central Prevailing Time.



Status:

Acknowledgment Required by **September 17, 2010**
Response Required by **October 15, 2010**



Private: Restrict to Internal Use and Necessary Consultants

Stuxnet is a very specialized piece of software that was designed to attack Siemens' Industrial Control Systems used to control high-speed electrical motors, like those used to spin gas centrifuges - one of the ways uranium can be enriched into bomb-grade material.

The software took advantage of five unknown vulnerabilities with Microsoft's operating system and print spooler program and was delivered using a flash drive

Threats - Duqu

TECHNOLOGY - SCITECH

Stuxnet Clone 'Duqu' Possibly Preparing Power Plant Attacks

By Matt Liebowitz

Published October 18, 2011 | TechMediaNetwork

Duqu, in effect, executes a reconnaissance mission by collecting design documents from an entity—critical industrial infrastructure components such as SCADA systems—to facilitate a future attack.

Key points from the report include:

- The executables share some code with the Stuxnet worm, and they were compiled after the last Stuxnet sample was recovered.
- There is no ICS specific attack code in the Duqu or infostealer.
- The primary infection vector for Duqu deployment has not yet been discovered/recovered (Duqu does not self-replicate or spread on its own).
- The targeted organizations appear to be limited.
- The malware employed a valid digital certificate (revoked as of October 14, 2011)
- The malware is designed to self-delete after 36 days.
- The Command and Control servers are hosted in India (Specific IPs unknown at this time).

SCADA and Industrial Control System Vulnerabilities

Italian researcher finds more SCADA holes

[Home](#) / [Blog](#) / [2011](#) / [May 2011](#) / [SCADA Vulnerabilities in Industrial Control Systems](#)

SCADA Vulnerabilities in Industrial Control Systems

May 18, 2011

By Rick Moy

Supervisory Control and Data Acquisition (SCADA) systems are cornerstones of modern industrial society. SCADA systems enable humans to control, monitor and automate activities of connected physical systems, such as oil and gas pipeline valves, temperature monitoring and cooling systems, energy grids, traffic lights, etc, Programmable Logic Controllers (PLCs) are the purpose-built devices that communicate with and control the physical devices. For example, they enable human operators to define rules that automatically turn on water cooling pumps to a nuclear reactor when the temperature reaches a predefined threshold. They are in use in every country and in every industrial control system, and impact our lives every day in ways we might not realize.

Continued discover of vulnerabilities

2011

[atvise webMI Web Server Multiple Remote Vulnerabilities](#)

[IRAI AUTOMGEN Buffer Overflow Vulnerability](#)

[Unitronics UniOPC Server Input Handling Vulnerability](#)

[InduSoft ISSSymbol ActiveX Control Buffer Overflow](#)

[Iconics GENESIS32 Multiple Memory Corruption Vulnerabilities](#)

[ARC Informatique PcVue HMI/SCADA Multiple ActiveX Vulnerabilities](#)

[Sunway ForceControl and pNetPower Multiple Security Vulnerabilities](#)

[Beckhoff TwinCAT 'TCATSysSrv.exe' Network Packet Denial of Service Vulnerability](#)

[Rockwell RSLogix Overflow Vulnerability](#)

[Measuresoft ScadaPro Multiple Vulnerabilities](#)

[Cogent DataHub Multiple Vulnerabilities](#)

[AzeoTech DAQFactory Stack Overflow](#)

[Progea Movicon Multiple Vulnerabilities](#)

[ScadaTEC ModbusTagServer and ScadaPhone Remote Buffer Overflow Vulnerability](#)

[Scadatec Procyon 'Coreservice.exe' Stack Buffer Overflow Vulnerability](#)

[Siemens WinCC Flexible Runtime Heap Overflow](#)

[Multiple ActiveX Vulnerabilities in Advantech Broadwin WebAccess](#)

[Sunway ForceControl SCADA SEH](#)

[Control Microsystems \(Schneider Electric\) ClearSCADA Remote Authentication Bypass](#)

[Inductive Automation Ignition Disclosure Vulnerability](#)

[Siemens SIMATIC S7-300 Hardcoded Credentials](#)

[Password Protection Vulnerability in Siemens SIMATIC Controllers \(S7-200,300,400,1200\)](#)

[Siemens SIMATIC S7-1200 PLC Vulnerabilities](#)

[Honeywell ScanServer ActiveX Control Use-After-Free Vulnerability](#)

2010

[Stuxnet \(Siemens PCS7/S7\)](#)

SCADA and Industrial Control System Vulnerabilities

Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

MIAMI, Florida — A group of researchers has discovered serious security holes in six top industrial control systems used in critical infrastructure and manufacturing facilities and, thanks to exploit modules they released on Thursday, have also made it easy for hackers to attack the systems before they're patched or taken offline.



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-020-01—S4 DISCLOSURE OF MULTIPLE PLC VULNERABILITIES IN MAJOR ICS VENDORS

January 20, 2012

Affected Vendors	Product
General Electric	D20/D20ME
Rockwell Automation	Allen-Bradley ControlLogix
Rockwell Automation	Allen-Bradley MicroLogix
Schneider Electric	Modicon Quantum
Koyo	Direct LOGIC H4-ES
Schweitzer	SEL-2032

Firmware					
Ladder Logic					
Backdoors					
Fuzzing					
Web			N/A	N/A	
Basic Config					
Exhaustion					
Undoc Features					

Chart listing the vulnerability types found in PLCs the researchers examined. A red "X" indicates the vulnerability is present in the system and is easily exploited; a yellow exclamation point indicates the vulnerability exists but is difficult to exploit; the green checkmark indicates the system lacks this vulnerability.

SCADA and Industrial Control System Vulnerabilities



No evidence of cyberattack at water pump, DHS says

From Mike Ahlers and Josh Levs, CNN
updated 10:21 PM EST, Tue November 22, 2011

STORY HIGHLIGHTS

• "No evidence of a cyber intrusion," the DHS says

(CNN) -- Federal investigators have found no evidence that a cyberattack was behind a water pump failure this month in Illinois, the government announced Tuesday.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT INFORMATION BULLETIN

ICSB-11-327-01—ILLINOIS WATER PUMP FAILURE REPORT

November 23, 2011

Reported cyber attack on water system in Illinois turned out to be false.

Initial details picked up by the media

- Pump Destroyed
- SCADA system vendor compromised and customer credentials stolen and used to access water system.
- Attack originated from Russia

Advanced Persistent Threats



HOMELAND SECURITY

Hackers reportedly have embedded code in power grid

April 08, 2009 | From Jeanne Meserve CNN



Computer hackers have embedded software in the United States' electricity grid and other infrastructure that could potentially disrupt service or damage equipment, two former federal officials told CNN.

The code in the power grid was discovered in 2006 or 2007, according to one of the officials, who called it "the 21st century version of Cold War spying."

Department of Homeland Security Director Janet Napolitano would not confirm such a breach, but said Wednesday that there has been no known damage caused by one.



The ex-officials say code also has been found in computer systems of oil and gas distributors.

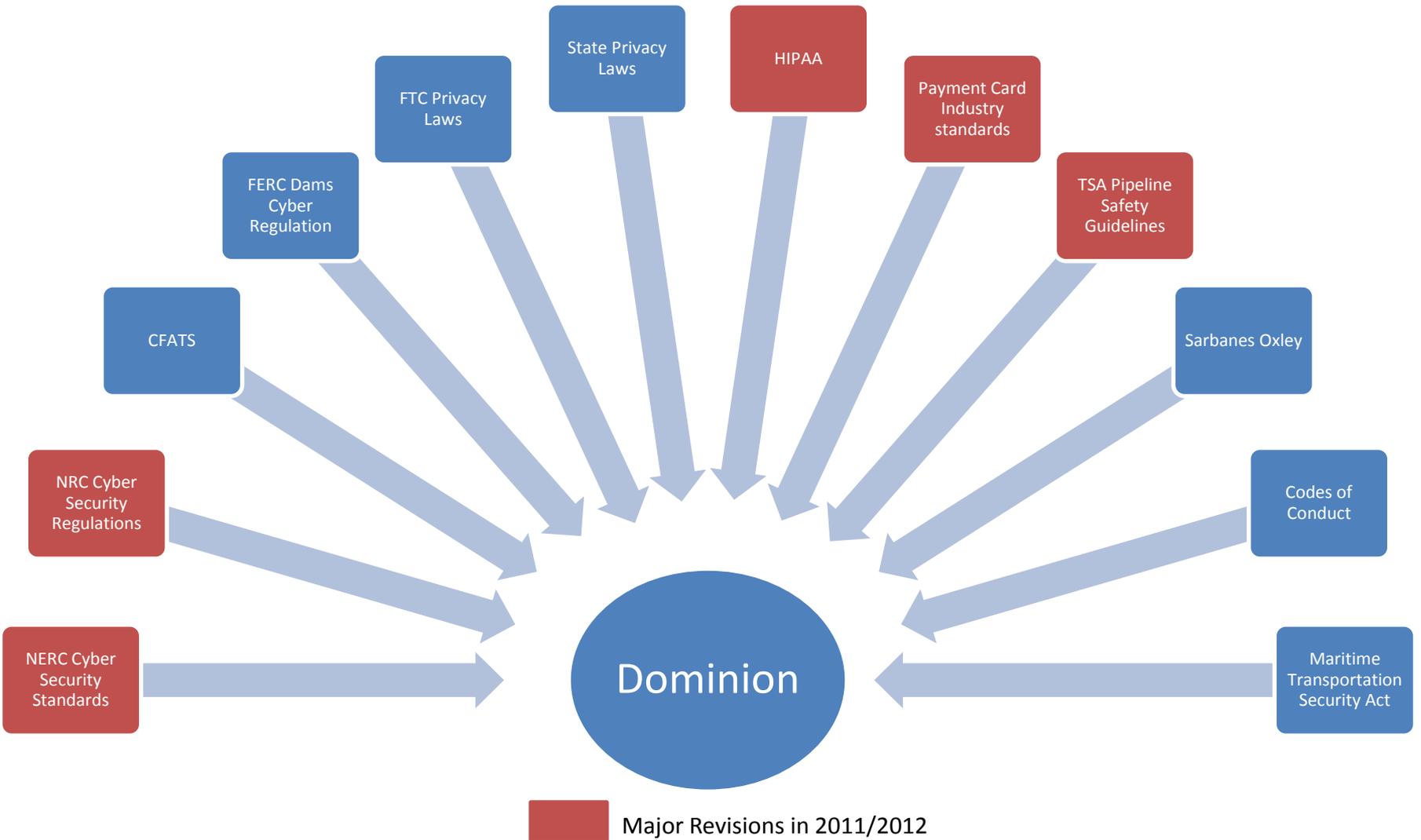
□ What is APT

- **Advanced Persistent Threats (APTs)** are a cybercrime category directed at business and political targets.
- APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful.
- The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached

Discussion Topics

- Brief Overview of Dominion
- Dominion's Cyber Security Program
- The Current Landscape
- Threats and Vulnerabilities
- **Regulatory and Legislative Update**

Cyber Security Regulatory Landscape



Administration – White House Proposal



- National Data Breach Reporting.
- Penalties for Computer Criminals.
- Voluntary Government Assistance to Industry, States, and Local Government.
- Voluntary Information Sharing by Industry, States and Local Government
- Critical Infrastructure Cybersecurity Plans.
- DHS Authority.
- Data Centers.

Legislative Activities

focusing on Process Control

- 44 pieces of legislation floating around Washington

Multiple hearings but no real movement

Legislation	Status
HR 76 – the Cybersecurity Education Enhancement Act of 2011	No Action
HR 174 – the Homeland Security Cyber and Physical Infrastructure Protection Act of 2011	No Action
HR 1136 – the Executive Cyberspace Coordination Act of 2011	No Action
HR 1261 – Chief Technology Officer Act	No Action
HR 2096 – the Cybersecurity Enhancement Act of 2011	Reported in House (112-264);
HR 3523 – the Cyber Intelligence Sharing and Protection Act of 2011	Pre-introduction hearing;

Legislation	Status
S 21 – Cyber Security and American Cyber Competitiveness Act of 2011	No Action
S 372 – Cybersecurity and Internet Safety Standards Act	No Action
S 413 – The Cybersecurity and Internet Freedom Act of 2011	Hearing Held 5-23-11
S 813 – the Cyber Security Public Awareness Act of 2011	No Action
S 1152 – the Cybersecurity Enhancement Act of 2011	No Action
S 1159 – the Cyberspace Warriors Act of 2011	No Action
S 1342 – the Grid Cyber Security Act	Reported in Senate (112-34)

Legislative Activities

Republican Proposals



Recommendations of the **House Republican Cybersecurity Task Force**

October 2011

- 1) Critical Infrastructure and Incentives
- 2) Information Sharing and Public-Private Partnerships
- 3) Updating Existing Cybersecurity Laws
- 4) Legal Authorities

The Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 (**The PrECISE Act**), **H.R. 3674**, authorizes the cybersecurity functions of the Department of Homeland Security (DHS),

- requiring DHS to conduct an evaluation of cybersecurity risks to critical infrastructure and determine the best mitigation methods.
- the legislation also establishes the **National Information Sharing Organization (NISO)**, a private-sector-controlled, not-for-profit organization to facilitate best practices, provide technical assistance, and enable the sharing of cyber threat information across critical infrastructure and with the federal government, while also protecting privacy and civil liberties.

White House / Department of Energy

Electric Sector Cybersecurity Risk Management Maturity Pilot Program

Program Description

The Electric Sector Cybersecurity Risk Management Maturity pilot program is a White House initiative that is being led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS) and in collaboration with volunteers from electric sector asset owners and operators.

Participants will design and draft a maturity model that reflects the key cybersecurity risk management performance elements for the electric sector and levels of maturity within each element.

For example, performance areas may include:

- supply chain,
- information sharing,
- threat awareness,
- incident management,
- cybersecurity workforce,
- standards, and
- continuous monitoring.

Desired Outcomes

- A cybersecurity risk management maturity model that is adopted by the electric sector and effectively used to characterize the current and evolving cybersecurity risk management capabilities within the electric sector (*deliverable – initial draft maturity model*)
- A snapshot of the cybersecurity risk management maturity for the pilot participants, based on their application of the model (*deliverable – non-attributable data*)
- Increased understanding of the electric sector’s risk management capabilities (*intangible*)

Dates	Activity
Nov – Dec 2011	Baseline relevant DOE, DHS, NERC, and other Electric Sector cybersecurity activities, resources, and capabilities
Dec 2011	Initiate industry engagement and solicit input to develop pilot program concept
Jan 5, 2012	Formal launch meeting with the White House, DOE, DHS, and ESCC (and industry CEOs)
Jan – Mar 2012	Confirm private sector participants and draft maturity model (phase 1)
Mar – Apr 2012	Pilot use of draft maturity model and obtain feedback (phase 2)
Apr – May 2012	Finalize draft maturity model and develop recommendations for expanded use by the sector (phase 3)

Securities and Exchange Commission Cyber Breach Reporting Guidelines



Home | Previous Page

U.S. Securities and Exchange Commission

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2
Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents

As with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

In November, [Consolidated Edison of New York](#), a large electric and gas utilities serving customers in [New York City](#) and Westchester County, included cyber-attacks as a risk factor that could affect investors quarterly report (10-Q) for the first time. Con [Edison's](#) 10-Q stated:

"A Cyber Attack Could Adversely Affect the Companies. The Utilities and other operators of [critical energy infrastructure](#) may face a heightened risk of cyber attack. In the event of such an attack, the Utilities and the competitive energy businesses could have their operations disrupted, property damaged and customer information stolen; experience substantial loss of revenues, response costs and other financial loss; and be subject to increased regulation, litigation and damage to their reputation."

Questions



Mark Engels
Director – Enterprise Technology Security and Compliance
Dominion Resources Services
Mark.Engels@dom.com



Application Testing using Random Data Patterns: or Fuzzing for Short

Bob Baskette
Senior Manager, Security Operations
and Architect



Fuzz Testing Background Info

- Software testing technique used to expose security issues in applications by introducing invalid, unexpected, or random data into the inputs of an application
- The application is monitored to detect process exceptions such as faults or failing built-in code assertions



Fuzz Testing Background Info

- The concept and term originates from a class project conducted at the University of Wisconsin Madison in 1989
<http://www.cs.wisc.edu/~bart/fuzz/>
- Fuzz testing is considered a Black Box testing technique since all testing is performed from an external view



Why Perform Fuzz Testing

- Fuzz testing is based on the assumption that coding errors exist within every application
- Fuzz testing can detect defects which may be overlooked by human testers due to the complexity of the application coding and will provide another point of view because Fuzz testing uses a non-human approach



Fuzzy Testing Targets

- Application code issues to be tested include:
 - Buffer overflows
 - Format strings
 - Code injections
 - Dangling pointers
 - Race conditions
 - Denial of service conditions

Fuzz Testing Targets

- File formats and network protocols are the most common targets of testing, but any type of program input can be Fuzz tested
- Interesting inputs include:
 - Environment variables
 - Keyboard and mouse events
 - Sequences of API calls
 - Contents of databases
 - Shared memory

Fuzzy Testing Targets

- Of primary importance is any input that crosses a trust boundary
 - It is more important to test code that handles the upload of a user's file than code used to parse a configuration file that is accessible only to a privileged user.
 - Any untrusted source of data input is considered to be insecure and inconsistent



Fuzz Testing Simple Example

- An application that records the selection between three items would use an integer to store a value between 0 – 2. The Fuzz test would determine what would happen if the application attempted to store a larger value than the integer could hold (buffer capacity) or a value not consistent with the application (logic issue)



Fuzz Testing Advantages

- Application errors uncovered by Fuzz testing can be severe, exploitable coding errors that could be used by a real attacker
- Fuzz testing can be used to uncover the same application issues used by malicious individuals since the same techniques and tools are now used by attackers to exploit deployed software



Fuzz Testing Advantages

- The greatest advantage of Fuzz testing is that the test conditions are extremely simple to design and that the test conditions are free of preconceptions about system behavior

Fuzz Testing Disadvantages

- The quality of the output is solely depended upon the quality of the input
- Catching a boundary value condition with random inputs is highly unlikely
- A Fuzz test may only verify that an application can handle exceptions without crashing, rather than behaving correctly



Fuzzy Analysis Common Steps

- Identify the target
- Identify inputs
- Generate Fuzz data
- Execute Fuzz data
- Monitor the output
- Determine the exploitability

Fuzz Testing Initialization

- It is important to configure the Fuzz testing tool to record the input data (including the pseudo-random number-generated seed value) to be used in the test to a file prior to executing the test.
- The file will be needed to reproduce the testing errors if the Fuzzing software causes the system to crash



Fuzz Testing Criteria Types

- Mutation-based
 - Fuzz testing that mutates existing data samples to create test data
- Generation-based
 - Fuzz testing that define new test data based on models of the input



Fuzz Testing Techniques

- A specification-based Fuzz Test involves writing the entire array of specifications into the tool
- The tool then uses model-based test generation techniques to walk through the specifications to add anomalies in the data contents, structures, messages, and sequences



Protocol-Based Fuzz Testing

- Protocol awareness can be used to generate Fuzz testing criteria and send forged packets to the target application
- The testing criteria can be generated from scratch, or the criteria can be mutated from examples from test suites or real data



Protocol-Based Fuzz Testing Limitations

- Testing will not be successful until the protocol specification is relatively mature since the specification is a prerequisite for writing the test condition
- Many useful protocols are proprietary or utilize proprietary extensions. If the test conditions are based only on published specifications the test results will be limited



Fuzz Testing Conditions/Vectors

- Define lists of "known-to-be-dangerous values" for each type
 - For integers: zero, negative, very big numbers
 - For chars: escaped, interpretable characters / instructions
 - For SQL Requests, quotes / commands
 - For binary: random ones



Application Fuzz Testing

- The attack vectors are within the I/O
- For a desktop application:
 - The UI (testing all the buttons sequences / text inputs)
 - The command-line options
 - The import/export capabilities (see file format fuzzing below)



Application Fuzz Testing

- The attack vectors are within the I/O
- For a web application
 - URLs
 - Forms
 - User-generated content
 - RPC requests



File Format Fuzz Testing

- Generates multiple malformed samples and processed the samples sequentially
- When the application generates a fault the debug information is kept for further investigation.



File Format Fuzz Testing

- Attack vectors include:
 - The codec/application layer
 - Lower-level attacks/ application internals
 - The parser layer (container layer)
 - File format constraints
 - File format structure
 - File format conventions
 - File format field sizes
 - File format flags



OWASP Information

- Open Web Application Security Project
- Does not focus on complete application security programs but provides a necessary foundation to integrate security through secure coding principles
- Application security includes the people, processes, management, and technology



OWASP Information

- The Open Web Application Security Project is a 501c3 not-for-profit worldwide organization focused on improving the security of application software
- The mission of OWASP is to make application security visible, so that organizations can make informed decisions about true application security risks



OWASP Top Ten

OWASP Top Ten project categorizes the application security risks by evaluating the top attack vectors and security weaknesses in relation to their technical and business impact

Each risk will demonstrate a generic attack method independent of the technology or platform in use



OWASP Top Ten

- A1 Injection
- A2 Cross-Site Scripting
- A3 Broken Authentication and Session Management
- A4 Insecure Direct Object References
- A5 Cross-Site Request Forgery



OWASP Top Ten

- A6 Security Misconfiguration
- A7 Insecure Cryptographic Storage
- A8 Failure to Restrict URL Access
- A9 Insufficient Transport Layer Protector
- A10 Unvalidated Redirects and forwards



Fuzz Testing software from OWASP

- WebScarab
 - Framework for analyzing applications that communicate using the HTTP and HTTPS protocols
- JBroFuzz
 - A stateless network protocol Fuzz testing program
- WSFuzzer
 - Real-world manual SOAP pen testing tool



JBrofuzz

- Well-known platform for web application Fuzz testing
- Supports both HTTP and HTTPS protocols
- Need to supply the URL and the part of the web request to Fuzz



JBrofuzz

- Can create a request manually or use a predefined set of payloads
 - Cross-site scripting
 - SQL Injection
 - Buffer overflow
 - Format String Error
- The responses will be recorded for tether inspection



JBroFuzz Application Overview

- Fuzzing Tab
 - The main tab of JBroFuzz
 - Responsible for all Fuzz testing operations performed over the network.
 - It creates the malformed data for each request depending on the payload selected and puts the data on the wire and writes the response to a file



JBroFuzz Application Overview

- Graphing Tab
 - Is responsible for graphing the responses received from the Fuzz test.
 - Provides a clear indication of a response that is different than the rest received
 - Generates a clear indication of further examination being required.



JBroFuzz Application Overview

- Payload Tab
 - A collection of Fuzz test with their corresponding payloads that can be used for the Fuzz test
 - Payloads are added to the request in the Fuzzing tab
 - Provides a clear view of what payloads are available, the properties of each payload and how the payloads are grouped for each test



JBroFuzz Application Overview

- Header Tab
 - A collection of browser headers that can be used while Fuzz testing
 - The headers are obtained from different browsers on different platforms and operating systems.
 - The headers are required since many web applications respond differently to different browser impersonation attacks.



JBroFuzz Application Overview

- System Tab
 - Represents the logging console of JBroFuzz at runtime
 - Can be used to access
 - Java runtime information
 - Errors that occur
 - Events being logged



Bunny

- General purpose Fuzz testing program designed specifically to test C programs
- Formulates the compiler-level integration which injects the instrumentation hooks into the application process and monitors its execution for changes in function calls, parameters, and return values in response to changes to the input data



Bunny

- Operation is performed in real-time and the feedback is provided accordingly
- Supports up to nine different fault injection strategies
- Provides detailed controls over the type, behavior, depth, and likeliness



Brute force Exploit Detector

- Tool designed to fuzz the plain-text protocols against potential buffer overflows, for-mat string bugs, integer overflows, and DoS conditions
- Automatically tests the implementation of a protocol by sending a different combination of commands with problematic strings to confuse the target



Brute force Exploit Detector

- BED protocols
 - FTP
 - SMTP
 - POP
 - HTTP
 - IMAP
 - PJJ
 - LPD
 - Finger
 - Socks4/Socks5



Fuzz Testing Summary

- Fuzz testing is intended to provide an assurance of overall quality rather than an end-all bug-finding tool
- Fuzz testing can suggest which parts of an application should get special attention
 - Code audit
 - Static analysis
 - Partial rewrites



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!



General Assembly Legislation Session 2012

Michael Watson
Acting Chief Information Security Officer



HB1149

Freedom of Information Act; electronic communication meetings by local and regional public bodies.

Freedom of Information Act; electronic communication meetings by local and regional public bodies. Expands the authority for the conduct of electronic communication meetings to all public bodies. Currently, local public bodies are prohibited from conducting public meetings in this manner, except when the Governor declares a state of emergency. The bill contains technical amendments. ***Patron: L. Mark Dudenhefer***

Status:

01/16/12 House: Presented and ordered printed 12102584D

01/16/12 House: Referred to Committee on General Laws

01/20/12 House: Assigned GL sub: #2 FOIA/Procurement



HB620

Information Technology and Management Internal Service Fund; established for VITA

Virginia Information Technologies Agency; internal service funds. Establishes the Information Technology and Management Internal Service Fund for the Virginia Information Technologies Agency. The newly established fund will replace the three funds currently administered by VITA. The bill also authorizes the Comptroller to establish, upon the request of the Chief Information Officer of the Commonwealth and the Joint Legislative Audit and Review Commission, other internal service fund accounts for receipts and expenditures of appropriate functions of VITA.

Patron: James M. LeMunyon

Status:

- 01/10/12 House: Prefiled and ordered printed; offered 01/11/12 12101866D
- 01/10/12 House: Referred to Committee on Science and Technology
- 01/25/12 House: Reported from Science and Technology (22-Y 0-N)
- 01/26/12 House: Read first time
- 01/27/12 House: Read second time and engrossed
- 01/30/12 House: Read third time and passed House BLOCK VOTE (99-Y 0-N)
- 01/30/12 House: VOTE: BLOCK VOTE PASSAGE (99-Y 0-N)



HB341

Auditor of Public Accounts; procurement of private accountants and auditing firms

Auditor of Public Accounts; procurement of private accountants and auditing firms. Requires the Auditor of Public Accounts to procure the professional services of CPAs and auditing firms to carry out his duty to audit all the accounts of every state department, officer, board, commission, institution or other agency handling any state funds, subject to the provision that the cost thereof shall not exceed such sums as may be available out of the appropriation provided by law for the conduct of his office.

Patron: Tony O. Wilt

Status:

01/10/12 House: Prefiled and ordered printed; offered 01/11/12 12102279D

01/10/12 House: Referred to Committee on Appropriations

01/16/12 House: Assigned App. sub: General Government

01/25/12 House: Subcommittee recommends laying on the table by voice vote



SJ15

Electronic identity credentials; JCOTS to study and determine possible liability concerns therewith

Study; JCOTS to study electronic security credentials; report. Directs the Joint Commission on Technology and Science to study electronic identity credentials and any possible liability concerns therewith. In conducting its study, the Joint Commission on Technology and Science shall (i) coordinate with stakeholders in both the public and private realm to identify opportunities, challenges, and strategies for the issuance of electronic security credentials; (ii) identify potential uses of electronic security credentials in transactions involving the Commonwealth; (iii) identify the role the Commonwealth should play in the issuance of identification documentation used by private electronic security credentialing services; (iv) identify policies and craft legislation that would facilitate the use and issuance of electronic security credentials; (v) identify and address through policies and legislation any liability considerations that may arise through the issuance of electronic security credentials by private entities; and (vi) consider such other related issues as the joint commission deems appropriate. JCOTS must report its final findings and recommendations to the 2013 Session of the General Assembly. **Patron: John C. Watkins**

Status: 01/04/12 Senate: Prefiled and ordered printed; offered 01/11/12
01/04/12 Senate: Referred to Committee on Rules



Virginia Information Technologies Agency

Upcoming Events





Security Training Offered

MS-ISAC Partnership Agreement with SANS Institute For Security Training

- **SANS Video Security Awareness Training -- Securing the Human:**
- Available online via SANS hosted site or SCORM-compliant for your own LMS
- Purchasing windows: **January 15, - February 29 & July 1, - July 31, 2012**
- To request a test account (one admin and three users) visit:
<https://www.securingthehuman.org/programs/ms-isac/>
- To register for the SANS purchasing portal to place your order during the purchasing window visit: <https://www.securingthehuman.org/programs/ms-isac/>

SANS Technical Training:

- OnDemand Group Flex Passes for Long Courses (4-6 days) and/or Short Courses (1-3 days)
- Universal Voucher Credits
- Purchasing window: **June 1 - June 30, 2012**



Coming: RFP for Security Training

VITA/CSRM developing RFP for

Security Awareness Training and Role Based Security Training

Objective

- to provide a COV contract vehicle for the purchasing of Security Awareness Training and Role Based Security Training.

RFP Team

- John Willinger, DBHDS
- Andrea Di Fabio, NSU
- Bob Auton, DJJ
- Ed Miller, VITA
- Benny Ambler, VITA

Time Frame

- April 2012 depending on the actual release date of the RFP and the number of bids received.



Kids Safe Online Poster Contest

2012 Cyber Security Awareness *Kids Safe Online* Poster Contest

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is conducting a 2012 national K-12 poster contest. The goal of the contest is to engage young people in creating posters to encourage other young people to use the Internet safely and securely. All public, private or home schooled students in kindergarten through 12th grade are eligible to participate.

The top three Virginia winners from each grade group (K-5, 6-8, 9-12) will be entered into the national competition. Entries received may be used in national, regional and state cyber and computer security awareness campaigns.

How to Enter: Schools may submit entries to the Commonwealth of Virginia competition by emailing submissions to CommonwealthSecurity@VITA.virginia.gov. A parent may submit for home schooled students. Please include the entry form completely filled out (all fields are required).

Commonwealth of Virginia submittals must be **received by February 23, 2012**. Winners of the Virginia contest will be automatically submitted to the national contest by March 1, 2012.

Entry Requirements:

Please see the <http://msisac.cisecurity.org/awareness/poster2012/> for entry form, requirements and judging criteria.

For more information or questions, please email CommonwealthSecurity@VITA.virginia.gov



IS Orientation Sessions

Tuesday - February 7, 2011

1:00 – 3:30p
(CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation is now available via webinar!



Information Security System Association

ISSA

DATE: Wednesday, Feb 8, 2012

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: *Symantec*

TOPIC: *Malware Trends and Techniques*



AITR Meeting

AITR Meeting:

Wednesday, February 8th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



COV IS Council

Commonwealth Information Security Council

Monday, February 27th, 12:00 - 2:00 p.m. @ CESC with
Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to CommonwealthSecurity@VITA.Virginia.Gov (no vendors please)

Find out more about your Commonwealth IS Council at:
<http://www.vita.virginia.gov/security/default.aspx?id=5128>



MS-ISAC Webcast

National Webcast Initiative

Wednesday, Feb 22

2:00 pm – 3:00 pm EDT

Topic: **Cyber Security Emerging Trends & Threats for 2012**

Visit MS-ISAC web for more information: <http://www.msisac.org/webcast/>



Training Offered

Intrusion Detection in Depth (SEC 503)

Host: Virginia Tech

Date: March 5-10, 2012 @ Virginia Tech, Blacksburg, VA

Who should attend?

- Intrusion detection analysts (all levels)
 - Network engineers
- System, security, and network administrators
 - Hands-on security managers

Discounts for state/local staff

(\$4200/pp normal rate, \$999/pp discount rate)!!

For More Info Visit: www.cpe.vt.edu/isect



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - March 7, 2011

Speaker: Dave Marcus, (McAfee) on Challenges in today's environment

Wednesday - April 4, 2012

Speaker: Laurie Jarrett (VCU) on Grant Writing basics

Upcoming:

May – Alana Foster with RSA

ISOAG will be held the 1st Wednesday of each month in 2012



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

February 1, 2012



NORTHROP GRUMMAN



ADJOURN

