Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 18, 2008

SEPTEMBER

ISOAG September 2008 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	InfraGard & Partners	Special Agent Melissa McRae, FBI
III.	Ongoing Security Awareness	Doug Mack, DMV
IV.	Disaster Recovery Services	Josh Haravay, VITA
V.	Center for Internet Security	Cathie Brown, VITA
VI.	Defending the Castle	Bob Baskette, VITA
VII.	Information Security Awareness Month	Nakita Albritton, VITA
VIII.	Cleaning Up SQL Injections	Michael Watson, VITA
IX.	Commonwealth Security Annual Report	Peggy Ward, VITA

NASCIO 2008 Finalists

The National Association of State CIOs, (NASCIO) has recognized the Commonwealth of Virginia as a finalist in 3 categories for excellence! See all submissions & finalists on the NASCIO Web site

www.nascio.org/awards

NASCIO 2008 Finalists

Categories & Commonwealth finalists are:

Information Security & Privacy

Commonwealth of Virginia - Information Security: Interlocking Spheres of Collaborative Protection

Enterprise IT Management Initiatives

Commonwealth Information Technology Infrastructure Partnership

Data, Information & Knowledge Management

Commonwealth of Virginia Knowledge Center

Losing the "T"

We are moving this year from Information "Technology" Security and "Cyber" Security to

Information Security!!

A comprehensive approach to information safeguards that includes ALL media such as the spoken word & hard copy documents as well as electronic media!

Information Security Awareness Month

Governor Kaine has signed a proclamation designating

October, 2008

as

Information Security Awareness Month

in the

Commonwealth of Virginia!!

2008 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials

Thank you MS-ISAC!

For printing cost estimates you can contact DMV's Damian McInerney @ 367-0925

Thank you DMV!

Thank You

InfraGard Program

Public and Private Sector Alliance Protecting our Critical Infrastructure

Melissa W. McRae

Special Agent

FBI Richmond, Cyber Squad

Paul Revere

Famous Midnight Ride of 1775

Israel Bissell

Four days and a total of 345 miles

Commemoration to Israel Bissell
Painting by H. W. Stark

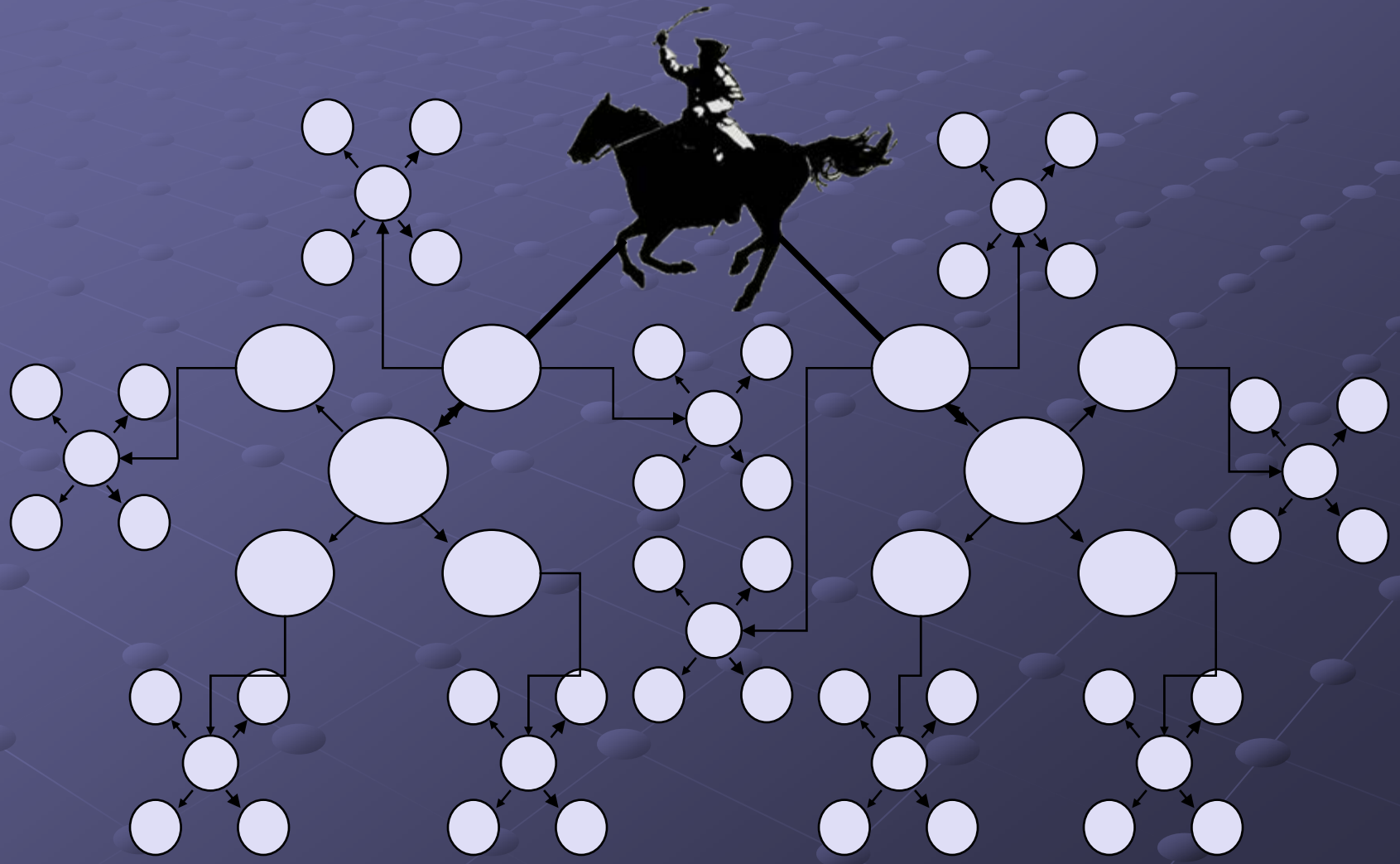
"Watertown,
To all friends of American Liberty be it known that this morning before break of day a Brigade consisting of about 1,000 or 1,200 men landed at Phip's farm at Cambridge and Marched to Lexington, where they found a company of our Colony Militia in Arms, upon whom they fired without provocation, and killed six men and wounded others. By an express from Boston we find that another brigade is now upon their march from Boston, supposed to be about 1,000. The bearer, Israel Bissell, is charged to alarm the country quite to Connecticut, and all persons are desired to furnish him with fresh horses, as they may be need."

Text from the letter carried by Israel Bissell from Watertown to Philadelphia

Networking

Rapid response system

Early warning system



A Brief History…

- In 1996, FBI Cleveland Field Office cyber focused industry outreach initiative.
- In 1998, the FBI adopted the InfraGard program for NIPC private sector outreach
- In 2003, the FBI Cyber Division was established and DHS formed taking NIPC mission.
- Today, InfraGard is the FBI's lead private and public sector information sharing tool

> 27,000 Members

National Critical Infrastructures

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

— *William J. Clinton, 1998*

Agriculture

Banking/Finance

Chemical

Computer Security

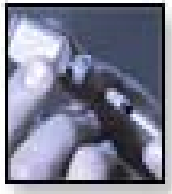
Defense

Emergency Service

Energy

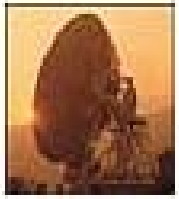
Food

Postal/Shipping

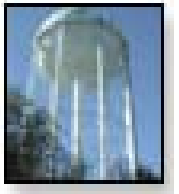


Public Health

Transportation



Telecommunication



Water Supply

Government Operations
Gas & Oil Storage and Delivery
Emergency Services
Water Supply Systems
Critical Infrastructures
Telecommunications
Banking & Finance
Electrical Energy
Transportation

InfraGard Benefits

FBI Program vs Private Sector

Benefits

- Trusted membership and Network of professionals
- Timely/Non-public Intelligence Products
- Secure forum to share information & discuss issues.
- Avenue to provide positive intelligence
- Ongoing relationship with the FBI

- Industry sector Subject Matter Experts
- Initiation of new investigations
- Early indication of sector specific attacks
- Avenue to obtain feedback on intelligence
- Ability to identify significant crime problems

Also, It is “FREE!”

Other Features

- **Secure website with FBI Alerts and Advisories, DHS Daily Reports**

Secure website with FBI Alerts and Advisories, DHS Daily Reports

- **Recent Alerts and Advisories**
  - Significant amount of Cyber related information due to program being under Cyber Division.
  - Other applicable Division information (e.g. Counterterrorism), however, is also posted.
- Items of Interest
- Recent News Articles
  - Sector Specific News
- Resource Page
  - DHS Daily Reports

Other Features

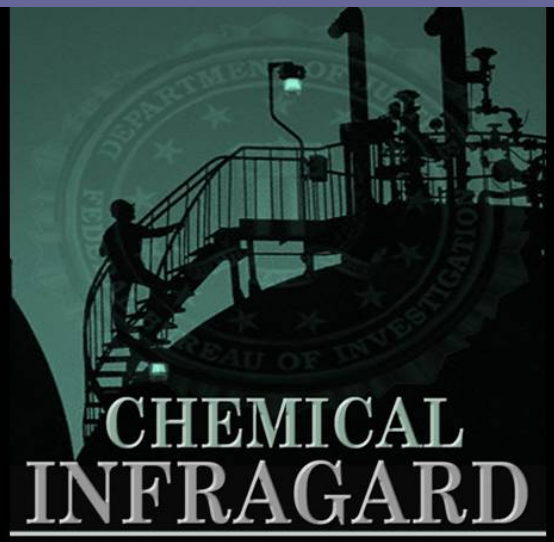
- Secure website with FBI Alerts and Advisories, DHS Daily Reports
- **Special Interest Groups**

Special Interest Groups

The Food/Agriculture InfraGard Special Interest Group (SIG) is a resource dedicated to the safeguarding of the food and agriculture sectors of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Food/Agriculture InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who can be called on to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the food and agriculture sectors of our nation's critical infrastructures. It aims to be a consortium of agriculture security professionals and law enforcement officials with the common goal of protecting America's farmland, food products, animals, and industry.

Participation in the Food/Agriculture InfraGard SIG requires membership in the national InfraGard Program and affiliation with the agriculture industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Food/Agriculture InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the agriculture industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the agriculture community are available to Food/Agriculture InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about food and agriculture sector issues in a secure environment. The site is also broken into areas specific to law enforcement, industry, food/agriculture agencies, animal/human health organizations and academia. The Food/Agriculture InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to agriculture-specific information sharing, driven to protect the food and agriculture infrastructure of the United States. To belong to the Food/Agriculture InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.



The Chemical InfraGard Special Interest Group (SIG) is a resource directed to the safeguarding of the chemical sector of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Chemical InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who may be called upon to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the chemical sector of our nation's critical infrastructures. It aims to be a consortium of chemical security professionals and law enforcement officials with the common goal of protecting America's chemical plants and industry.

Participation in the Chemical InfraGard SIG requires membership in the national InfraGard Program and affiliation with the chemical industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Chemical InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the chemical industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the chemical community are available to Chemical InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about chemical sector issues in a secure environment. There is also a Chemical InfraGard SIG listserv which allows SIG moderators the ability to correspond upcoming events and important announcements directly to SIG members via secure e-mail. The Chemical InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to chemical-specific information sharing, driven to protect the chemical infrastructure of the United States. To belong to the Chemical InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.

The Research and Technology Protection InfraGard Special Interest Group (SIG) is a resource dedicated to the safeguarding of our new and developing technologies from illegal acquisition by foreign adversaries. Although innovation in the United States benefits from a globalized economy, these international relationships make our technology increasingly vulnerable to foreign adversaries covertly acquiring and illegally transferring U.S. technology including proprietary information and trade secrets. The Research and Technology Protection InfraGard SIG enhances the efforts to protect research and technology made by private industry, academia and government through information-sharing networks with a private secure portal of communication.

The Research and Technology Protection InfraGard SIG is a collaborative effort of the Foreign-Counterintelligence and Cyber Divisions of the FBI. It is intended to enhance the sharing of information among private sector stakeholders who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting the innovation that drives our national economy. It is the consortium of members representing U.S. firms, universities, national laboratories, sensitive government facilities and law enforcement with the common goal of protecting our country's research and technology.

Participation in the Research and Technology Protection InfraGard SIG requires membership in the national InfraGard Program and affiliation with the scientific and technological research and development fields. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Research and Technology Protection InfraGard SIG by submitting an e-mail containing answers to questions about the member's association with these fields.

Assessments, news, relevant links and up-to-date information on protection issues related to the research and technology communities are available to Research and Technology Protection InfraGard SIG members. This is a unique opportunity for you to belong to the fastest growing information-sharing network dedicated to research and technology protection.

Other Features

- Secure website with FBI Alerts and Advisories, DHS Daily Reports
- Special Interest Groups
- **Information on seminars, training, other resources (Fusion Ctr, IC3, NCFTA, etc…)**

Virginia State Police

http://www.vsp.state.va.us/FusionCenter/index.shtm

Virginia.gov Online Services | Commonwealth Sites | Help | Governor

Search Virginia.gov GO

Virginia Fusion Center

Home

- About Us
- 7 Signs of Terrorism
- Terrorism Information
- Report Suspicious Activity
- Related Web Links
- National Threat Level

ELEVATED

Suspicious Incident Report

The Virginia Fusion Center was created to improve the Commonwealth of Virginia's preparedness against terrorist attacks.

The Center is essential to Virginia's homeland security efforts and is the primary resource for exchanging critical information among local, state and national homeland security, law enforcement and intelligence agencies.

The Cost of Freedom, Fighting Terrorism.
Discovery Education (2004).
CLOSED CAPTION VERSION

REPORT SUSPICIOUS ACTIVITY

Information regarding suspected terrorism activity or suspicious incidents should be reported to:

Toll Free Terrorism Hotline
877- 4VA-TIPS (877- 482- 8477)

OR

Suspicious Incident Report

877- 4VA-TIPS (877- 482- 8477) | Report Suspicious Activity | Privacy Policy | WAI Level A Compliant | All rights reserved, VSP & VDEM, 2007

INTERNET CRIME COMPLAINT CENTER

... an FBI - NW3C Partnership

Welcome to IC3

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes. read more >>

Filing a Complaint with IC3

IC3 accepts online Internet crime complaints from either the person who believes they were defrauded or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were

IC3 Flyer

IC3 Safety Poster

INTERNET CRIME COMPLAINT CENTER

... an FBI - NW3C Partnership

IC3's Public/Private Alliances

In addition to the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI), a number of other agencies have provided added value to the Internet Crime Complaint Center (IC3) project in the form of staffing, recommendations, and other support. IC3 is taking aggressive steps to exponentially strengthen law enforcement's ability to identify and combat Internet crimes. New and expanded alliances with industry is a key component to making Internet e-commerce safer for consumers. Association with these industry partners will allow the IC3 to capitalize on the information and intelligence received from industry partners to ensure significant cases are developed and referred to law enforcement in an expeditious fashion. Among these are:

BUSINESS SOFTWARE ALLIANCE (BSA)

The Business Software Alliance (BSA) was founded in 1988 and includes members throughout the world who are part of the high-tech industry. BSA promotes policy, education, and intellectual enforcement efforts on behalf of its members.

DIRECT MARKETING ASSOCIATION (DMA)

The Direct Marketing Association (DMA), founded in 1917, represents businesses interested in direct, database, and interactive global marketing. The DMA's membership includes companies from the United States and 44 foreign nations. The DMA works to encourage the education, growth and profitability of members through direct/interactive marketing methods.

NATIONAL CYBER-FORENSICS & TRAINING ALLIANCE (NCFTA)

The mission of the National Cyber-Forensics & Training Alliance (NCFTA) is to provide a neutral, collaborative venue where critical, confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia, and law enforcement. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations which are all intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

NIGERIAN ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC)

The Nigerian Economic and Financial Crimes Commission (EFCC) strives to combat economic and financial crime through cooperative working relationships with established enforcement and regulatory agencies. The Commission is empowered to prevent, investigate, prosecute, and penalize economic and financial crimes and is charged with the responsibility of enforcing the provisions of other laws and regulations relating to economic and financial crimes.

REPORTING ECONOMIC CRIME ON-LINE (RECOL)

Reporting Economic Crime On-Line (RECOL) is administered by the National White Collar Crime Center of Canada (NW4C) and is supported by the Royal Canadian Mounted Police and other participating agencies. RECOL involves an integrated partnership between international, federal, and provincial law enforcement agencies, as well as with regulators and private commercial organizations that have a legitimate investigative interest in receiving complaints involving economic crime.

UNITED STATES POSTAL INSPECTION SERVICE (USPIS)

The United States Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service. Postal Inspectors enforce over

National Cyber-Forensics & Training Alliance

http://www.ncfta.net/default2.asp

Site protected by:
VIGILANTMINDS

National Cyber-Forensics & Training Alliance

The National Cyber-Forensics and Training Alliance provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement.

The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations.

These activities are intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

Objectives
NCFTA will bring together local, state, and federal law enforcement, businesses, and academic institutions to functionally collaborate on cybercrime issues.

It will establish jointly developed and staffed facilities, where program participants will benefit from cyber-forensic analysis, tactical response development, technological simulation/modeling analysis, and the development of advanced training.

TOP ALERTS

- Micro Deposits
- Limbo 2 Trojan
- BlackBerry Users at Risk
- Phantom Merchants
- UPS Spam Trojan
- The Coreflood Trojan
- Silentbanker Trojan Strikes Again
- Malware Infected Multimedia Files
- Malware Plays on Olympic Games
- Turkish Botnet Infects Cartoon Fans

view all scams / threats

NEWS & RESEARCH

8/29/2007
Cyber-Security Issues: Congressional Testimony
Good afternoon Chairman Akin, ranking member Bordallo, and members of the committee .... *read more*

Other Features

- Secure website with FBI Alerts and Advisories, DHS Daily Reports
- Special Interest Groups
- Information on seminars, training, other resources (Fusion Ctr, IC3, NCFTA, etc…)
- **Valuable speakers at meetings**

InfraGard

InfraGard Member Alliance of Richmond, Virginia

Notice of Training Session–

Introduction and Use of the

National Incident Management System (NIMS)

September 20, 2007

8:00 AM – 12:00 PM

Commonwealth Enterprise Solutions Center, Chester, VA

The NIMS system is a federally mandated Emergency Management requirement for use by Public and Private Entities throughout the nation. In association with the Commonwealth of Virginia and our regional localities, the Richmond Member Alliance of Infragard is proud to sponsor this training for local corporations and all entities that would be affected by a regional response to a major disaster. The training will include an overview of the following:

- Regional Emergency Management Structure
- Emergency Preparedness for Employees and Corporate Administration
- Incident Command System
- Business Continuity Planning
- FEMA's IS Emergency Management Courses
- Table Top Exercises

Training Conducted by the Virginia Office of Commonwealth Preparedness
And the Regional Localities

Please RSVP to Bobby Vaughan at bobby.vaughan1@infragard.org by no later than September 10, 2007. Attendance is free and limited to two per company.

You will need to bring a valid ID for vetting at the entrance.

Richmond InfraGard

Chapter Meeting
December 12, 2007

Topic:
Threats to the Food/Agriculture Sector

Hosted By: Philip Morris
Time: 10 am to noon (registration beginning at 9:30 am)
Location: PMUSA Center for Research and Technology (CRT)
601 East Jackson St, Richmond VA 23219
RSVP: melissa.mcrae@infragard.org

InfraGard

InfraGard Richmond Virginia

Meeting – May 19, 2008
Chemical Security Legislation - CFATS

Time: 1:00 PM – 3:00 PM
VCU Engineering and Business School
Snead Hall, Room B1115
301 W. Main St, Richmond, VA 23284

Main Speakers:

Mr. Christopher Krebs
Senior Policy Advisor to the Assistant DHS Secretary for Infrastructure Protection

Mr. Evan Wolff
Director, Homeland Security Practice, Hunton and Williams LLP

Opening Remarks:

Mr. John Donahue, Richmond Infragard Council

SA Melissa McRae, FBI Richmond Field Office, Richmond InfraGard Coordinator

SAC Jennifer Love, FBI Richmond Field Office

SSA Brian Crews, FBIHQ InfraGard

Please RSVP As Soon As Possible to Ed Martella at 804-217-8504 or at
EFMartella@tectonicengineering.com
You will need to bring a valid ID for vetting.

Information Security Management

International Federation for Information Processing
www.ifip.org

Protecting Your Trade Secrets!

It’s been protected for over 100 years!

What's a "Trade Secret"?

Defined at 18 U.S.C. 1839:

- Must be not generally known to public;
- Steps to protect the information must be commensurate with the value of the trade secret (physical security, computer security, licensees);
- Must have independent economic value;
- Must be related to a product

FBI Citizens' Academy

- Two slots reserved for InfraGard members in every Richmond Citizens' Academy Class.

InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI)

http://www.infragard.net/

Google

InfraGard®

a collaboration for infrastracture protection

- HOME
- ABOUT INFRAGARD
- BECOME A MEMBER
- FIND YOUR CHAPTER
- NEWS ROOM
- LINKS
- CONTACT

SPECIAL INTEREST GROUPS

29-Aug-2008

27,165 MEMBERS (Including FBI)

LEARN MORE ABOUT INFRAGARD®

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Learn more about InfraGard

IN THE NEWS

- **The International Association of Campus Law Enforcement Administrators (IACLEA)**

ELEVATED
significant risk of terrorist attacks

BECOME A MEMBER

APPLY FOR MEMBERSHIP

Attend a local chapter meeting, meet FBI officials from your area, and help protect your nation's infrastructure today.

INFRASTRUCTURE PROTECTION

It is our goal to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.

FEATURED CHAPTER

NATIONS CAPITAL

InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.infragard.net/chapters/index.php?mn=3 Go

InfraGard®

a collaboration for infrastructure protection

- HOME
- ABOUT INFRAGARD
- BECOME A MEMBER
- FIND YOUR CHAPTER
- NEWS ROOM
- LINKS
- CONTACT

SPECIAL INTEREST GROUPS

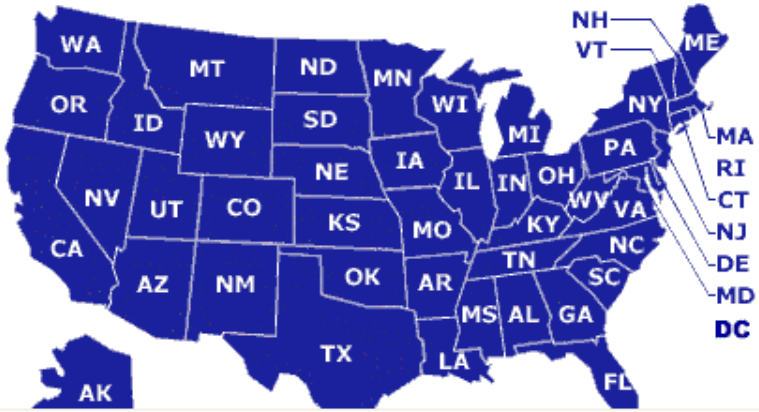
02-Jun-2008 24,582 MEMBERS (Including FBI)

Home | Find Your Chapter

FIND YOUR CHAPTER

Chapters are affiliated with 56 field offices in the FBI.

Please choose your state:



Rhode Island Internet

InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.infragard.net/chapters/page.php?mn=3&page=files/virginia.htm Go

InfraGard®

a collaboration for infrastructure protection

- HOME
- ABOUT INFRAGARD
- BECOME A MEMBER
- FIND YOUR CHAPTER
- NEWS ROOM
- LINKS
- CONTACT

SPECIAL INTEREST GROUPS

02-Jun-2008 24,582 MEMBERS (Including FBI)

Home | Chapters

Virginia

DC Metro Area

Norfolk

www.infragard-va.org

Richmond

Done Internet

InfraGard – Richmond, VA Chapter

http://www.infragard.net/chapters/richmond/

InfraGard®

Richmond, VA

- RICHMOND HOME
- MEETINGS
- MEMBERSHIP
- EXECUTIVE BOARD
- OTHER CHAPTERS
- INCIDENT REPORTING
- INFRAGARD HOME
- SPECIAL INTEREST GROUPS

29-Aug-2008

Home | Find Your Chapter | **Richmond, VA**

Welcome to Richmond, VA InfraGard Chapter

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.

This web site is specifically designed to facilitate the activities of the InfraGard chapter of Richmond.

InfraGard®
Richmond, VA

29-Aug-2008

Meetings

May 19, 2008

The next Richmond InfraGard Chapter meeting will be on May 19, 2008 from 1pm to 3pm. It will be held at Virginia Commonwealth University (VCU) in their new Engineering and Business School building, Snead Hall, Room B1115. The building is located at the intersection of Main St and Belvedere, just before you get to Cary St. It is located on the East side of Belvedere. and the address is 301 W. Main St, Richmond, VA 23284.

The focus of the meeting will be on the new Chemical Security Legislation, CFATS. In addition to the main speakers, who will be speaking about CFATS, we will also have a panel of experts in WMD and Export Control who will be available for a question/answer session. Please see the link below for additional information regarding this meeting.

Please extend the invitation to anyone else in your organization or outside your organization who would benefit from this meeting. Please note that all attendees must bring a valid ID for vetting

Federal Bureau of Investigation

Richmond, Virginia

(804) 261-1044

www.InfraGard.net

Ongoing Security Awareness

Douglas G. Mack

DMV IT Security Director (ISO)

Douglas.Mack@dmv.virginia.gov

(804) – 367 - 2221

ISOAG Meeting September 18, 2008

- September is **Internet Safety Month.**
- October is **Cyber Security Awareness Month.**
- What about the other **10 Months** of the year?

“Information security is a **people**, rather than a technical, issue.”

Mark B. Desman

The Ten Commandments of Information Security Awareness Training

What do we do?

Develop a Security Mindset

- Security becomes “second nature.”
  - Example: Telephone Call.
- Able to apply “general” principles to “specific” situation.
  - Example: Phishing Email.

How do we Develop a Security Mindset ?

- The two “R’s”
  - Recognition
    - Help Folks to see the need for security.
  - Reinforcement
    - Continually bring security to their attention.

How do we Address the Two “R’s?”

- By providing Ongoing Security Awareness Training.

General “Principles”

General “Principles” for Ongoing Security Awareness Training

- Make it “Alive/Engaging/ Memorable” rather than “Dull/Boring/Forgettable.”
- Make it “Personal.”

Dull/Boring/Forgettable

Good afternoon agency users,

Please remember to change your password regularly.

Also, please do not share your password with others.

Thanks!

Alive/Engaging/Memorable

**Your password is like a toothbrush;
use it regularly, change it often,
and do not share it with anyone else.**

Alive/Engaging/Memorable

Passwords are like bubble gum:

Strongest when fresh.

Should be used by an individual, not a group.

If left laying around, will create a sticky mess.

Make it “Personal”

- Address Work related issues <u>and</u> Home related issues.
  - Firewalls
    - The role they play at work
    - Need for them at home and what some of the options are
  - Protecting your children on the web

Specific Ideas

Specific Ideas

- Information Security Notes
- Information Security Alerts
- Small Group Presentations
- Small Posters
- Signature Line

Information Security Notes

- Single Topic
- Humorous/Fun
- Diagrams, Screen Prints, Pictures
- Put on Intranet
- Send Email to Users telling them of the New Security Note – include a Link

Information Technology (IT) Security Note # 5 - Pirates on the James River?

2/25/2008

Good morning DMV,

No, Captain Jack Sparrow (Johnny Depp) is not sailing up the James River! But, we may know a software pirate or two (or more)!

Software piracy is a growing issue that has serious consequences not only for the software developers/publishers but for government, companies, and individual users.

What is software piracy? Microsoft gives us a very good definition of software piracy when they write,

"Software piracy is the theft of software through illegal copying of genuine programs or through counterfeiting and distribution of imitation software products

Information Technology (IT) Security Note # 16 – Vacation Puzzle

6/25/2008

Good morning DMV,

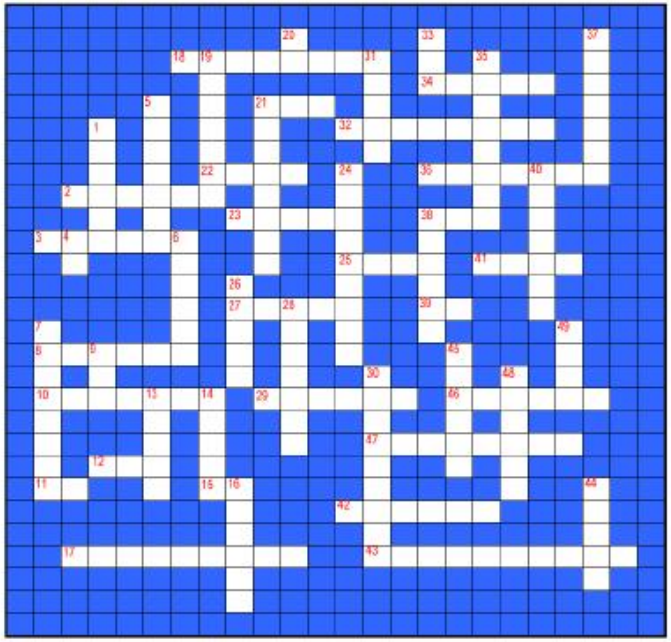
Summer is well underway, and the Fourth of July is next week!

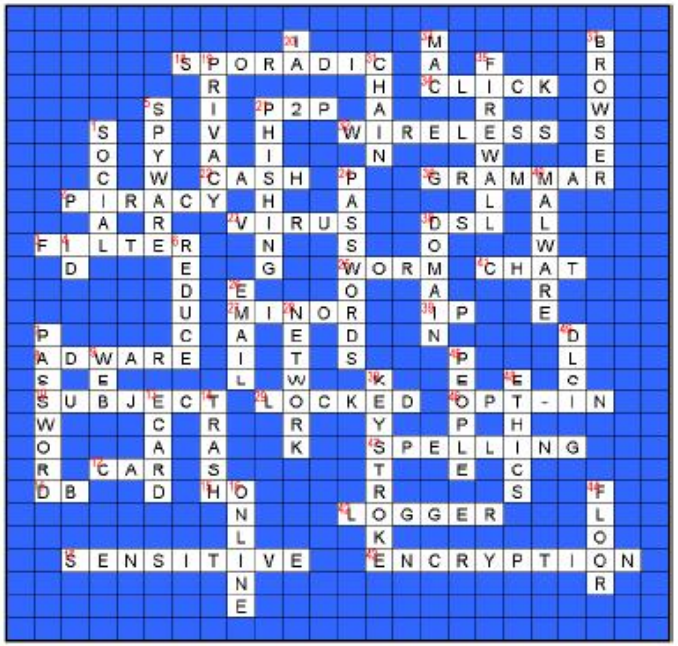
Security, of course, doesn't take a break for the summer. But, that's not to say we can't have a bit of fun with it!

An IT Security Puzzle and clues are on the following pages.

With only a few exceptions, the answers for the puzzle are taken from previous IT Security Notes. The answers that are exceptions are taken from DMV's external and internal web sites.

1	Down	_____ engineering is referred to as an approach to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals.
2	Across	Software _____ is the theft of software through illegal copying of genuine programs or through counterfeiting and distribution of imitation software products or unauthorized versions of software products.
3	Across	A software _____ screens information on the internet, classifies its content, and allows the user to block certain kinds of content.
4	Down	Don't share your user <4> or <7 Down> .
5	Down	_____ is a software program that may be installed on your computer without your consent to monitor your use, send pop-up ads, redirect your computer to certain websites, or record keystrokes, which could lead to identity theft.
6	Down	To _____ the amount of spam you receive, be careful who you give your email address to.
7	Down	Don't share your user <4 Down> or <7> .
8	Across	_____ is a type of software that often comes with free downloads. Sometimes it displays ads on your computer, while some monitors your computer use (including websites visited) and displays targeted ads based on your use.
9	Down	DMV does block certain specific individual sites.
10	Across	Always include a clear and specific line in your email.
11	Across	__ is the Commissioner of DMV.
12	Across	How to keep your laptop safe: Get it out of the ___ . . . don't ever leave it behind.
13	Down	_____ web sites provide an easy method for the "harvesting" of email addresses – which leads to more spam in our mailboxes.
14	Down	Before you throw something in the _____, ask yourself, "Is





		instantly on the screens of others who are in the room.
42	Across	A __<30 Down>____ <42>_ is a device or program that records each keystroke typed on a particular computer.
43	Across	_____ is the scrambling of data into a secret code that can be read only by software set to decode the information.
44	Down	How to keep your laptop safe: Keep it off the ____ . . . or at least between your feet.
45	Down	PEAK = _<45>_, _<48 Down>_, Accuracy and Knowledge.
46	Across	_____ is when a user explicitly permits a website to collect, use, or share his or her information.
47	Across	Always check your __<47>__ and _<36 Across>_ in your email before sending it.
48	Down	PEAK = <45 Down> , <48> , Accuracy and Knowledge.
49	Down	____ [abbreviation] is primarily responsible for providing driver's licenses to the citizens of the Commonwealth of Virginia.

Where can you get Content and Design?

- Write/Design it Yourself
- Partner with other ISOs
- Use Resources (observe copyright restrictions)
  - VITA's *Information Security Tips*

Where can you get Content and Design?

- More Resources
  - Federal Bureau of Investigation (FBI)
    - www.fbi.gov
  - Search Security
    - www.searchsecurity.com

Where can you get Content and Design?

- More Resources
  - Central Coast Security
    - http://members.impulse.net/~safe/aboutus.html
  - World Start
    - www.worldstart.com

Information Security Alerts

- Respond to Specific Incident/ Issue.
  - Example: PayPal & Langley FCU Phishing Attempts in May
- Send Email to Agency Users with Specific Information.

Small Group Presentations

- Departments/Work Groups
- Can range from 10/15 minutes to an hour.
- Basic Information Security Topics
  - How to create a good password
  - Email attachments that are blocked

Small Group Presentations

- More Basic Information Security Topics
  - Policy on personal use of computer equipment
  - Define sensitive data
  - Using encryption to send sensitive data
- Ripple Effect

Small Posters

8 ½ x 11 Inch Posters

Your password is like a toothbrush; use it regularly, change it often, and do not share it with anyone else.

Passwords are like bubble gum:

Strongest when fresh.

Should be used by an individual, not a group.

If left laying around, will create a sticky mess.

Small Posters

8 ½ x 11 Inch Posters

Signature Line

- Simply adding a Security Phrase to your Signature keeps “security” in front of folks.
  - Douglas G. Mack
    IT Security Director (ISO)
    Virginia Department of Motor Vehicles
    (804) – 367 – 2221
    SEC_RITY is not complete without U!

Final Thoughts

- Spread the Word about Information Security.
- Do it Often and Everywhere.
- Have Fun Doing It!

Disaster Recovery Services

Expanded Services

Joshua Haravay, VITA Disaster Recovery Specialist

September 18, 2008

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Agenda

- Objective and Goals
- DR Service Catalog
- Architecture and Proposed Tier Architecture
- Agency Requirements Gathering and DR Tier Mapping
- Other Services
- Questions

Objective and Goals

- Provide an overview of the Services that will be offered under the DR Services Catalog.
- Provide an overview of the solution that falls under a tier level of DR service
- Provide an understanding of the criteria used to help map an agency to a DR Service Tier
- Provide an overview of other available DR Services

Advantages of DR Services Catalog

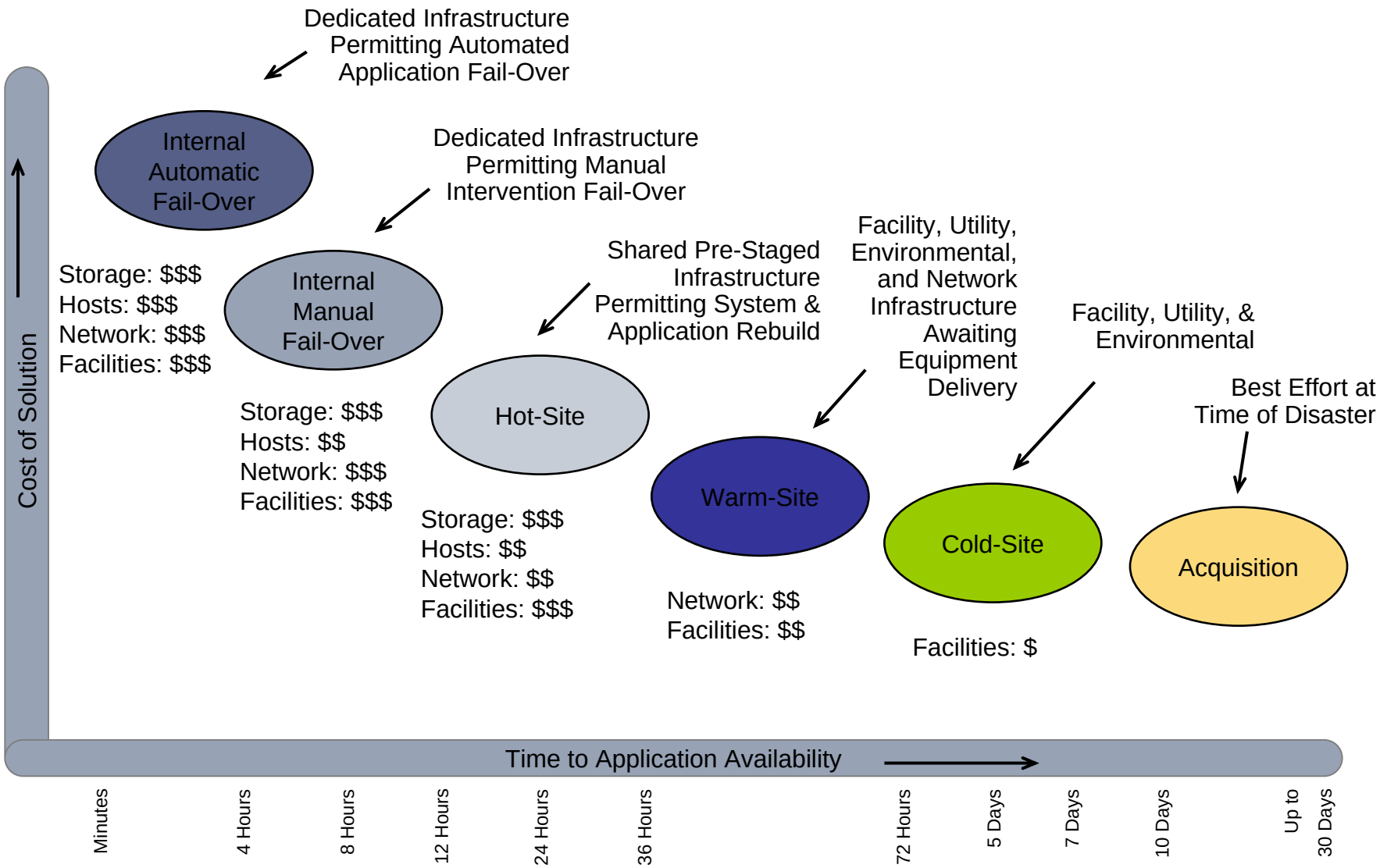
- Provides more granularity on costs of services for the Agencies
  - Agencies can choose between a larger range of services and choose the most applicable for their case
  - Agencies can select lower DR levels with lower costs
  - Agencies can match the solution to their RTO/RPO requirements
- Offers support for immediate needs of the Agencies
  - Agencies desire DR support for their local IT
  - Some Agency ITs cannot have SAN infrastructure
- Provides a logical migration path for the Agencies

Disaster Recovery Service Measures

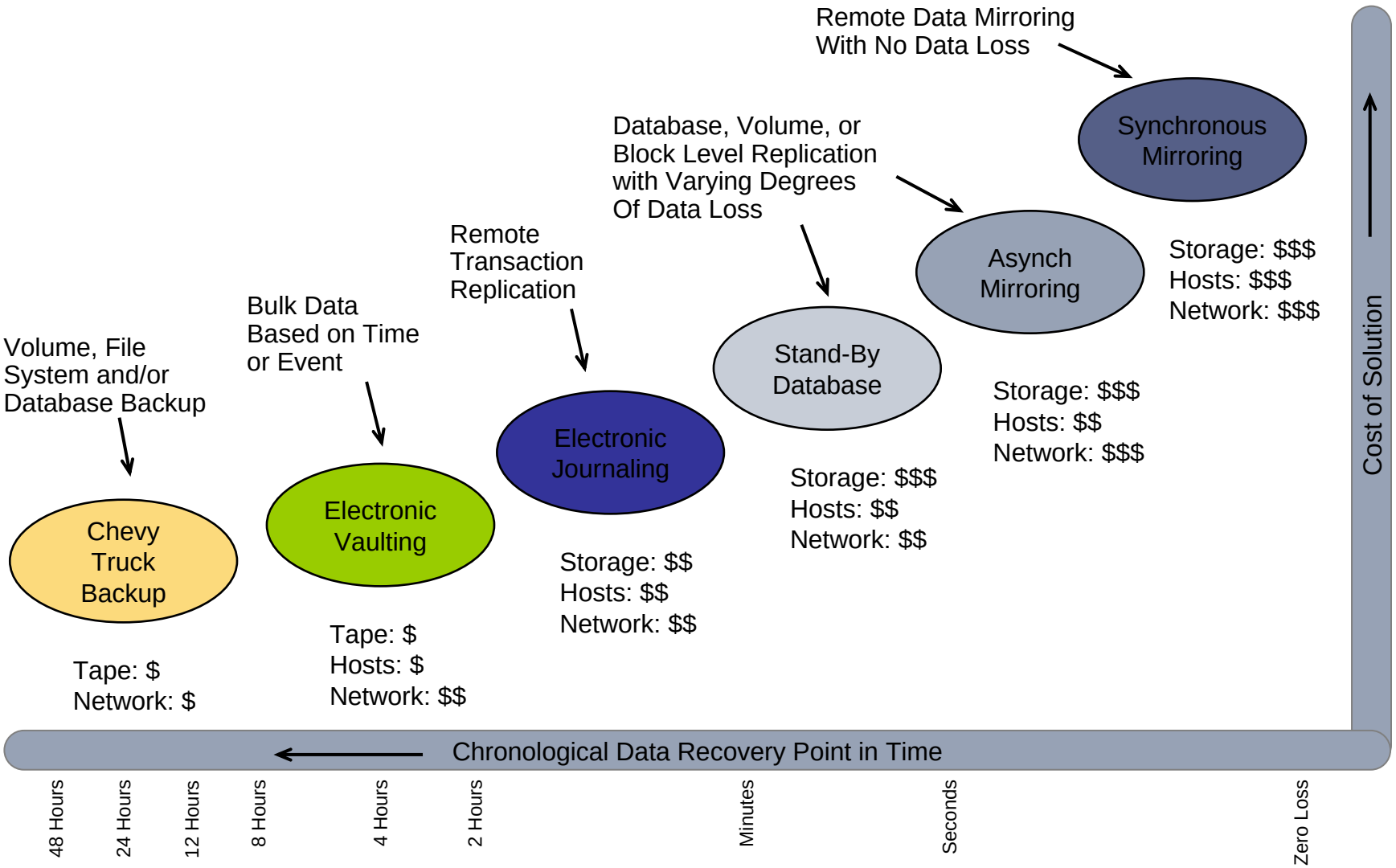
Definition	Time to recover the affected Commonwealth Services after a declared DR incident

Disaster Recovery Service Level Requirements			
BIA Application Rankings	**Service Measure**	**Performance Target**	**Minimum Performance % ALL SOWs**
1	Time to recover	< 4 hours	98%
2	Time to recover	5 to 24 hours	98%
3	Time to recover	25 to 48 hours	98%
4	Time to recover	49 to 72	98%
5	Time to recover	>73 hours	98%
6	Time to recover	Within 168 hours	100%

Delivering Degrees of RTO



Delivering Degrees of RPO



Gartner

Disaster Recovery Service Reference Architecture		Tier 1 <4 hrs	Tier 2 5 – 24 hrs	Tier 3 25 – 48 hrs	Tier 4,5,6 49 – 72 hrs > 73 hrs Within 168 hrs
Servers	**Server Type**	Physical	Physical / Virtual	Physical / Virtual	Physical / Virtual
	Clustering	Optional	Optional	Optional	N/A
	Continuous Availability	Optional	Optional	Optional	N/A
	High Availability	Optional	Optional	Optional	N/A
	Type of Clustering	Active / Active Active / Passive	Active / Active Active / Passive	Active / Active Active / Passive	N/A
	Server Status DR Site	Dedicated	Repurposed or Dedicated	Repurposed or Dedicated	Drop Ship or Repurposed or Dedicated
	Storage Type	SAN	SAN	SAN	SAN / DAS / Local
	Server Operational Recovery Method	High Availability	High Availability or Rebuild	Rebuild	Rebuild
	Host Bus Adaptors Required (minimum)	1	1	1	0
	Network Interface Cards Required (minimum)	1	1	1	1
Storage	Storage Frame	Enterprise level High End	Enterprise level High End	Enterprise level High End	Mid-Range
	Storage Type	SAN	SAN	SAN	SAN / DAS / Local
	Data Replication	Array-based	Array-based	Backup	Backup
	Type of Replication	Asynchronous	Asynchronous	Restore from Disk	Restore from Tape
	Replication Bandwidth Required	Dependent on Application	Dependent on Application	Dependent on Application	N/A
	Switch Fabric Connections	2	2	2	1
	Frequency of Data Replication	<=4 Hours	<=4 Hours	<=24 Hours	<=24 Hours
	Data Copies – Production	Variable	Variable	1	N/A
	Data Copies – DR Copy	Variable	Variable	1	N/A
	Data Copies – Backups	Optional	Optional	Weekly full copy and daily incremental	Weekly full copy and daily incremental
	Data Protection – Production	RAID 10	RAID 10	RAID 10	Optional
	Data Protection – DR Gold Copy	Parity RAID	Parity RAID	N/A	N/A
	Data Protection – Backup	Optional	Optional	Disk based	Tape based
	Continuous Data Protection	N/A	N/A	N/A	N/A
	Continuous Remote Replication	N/A	N/A	N/A	N/A
	Operational Recovery Method	BCV / Clone / Snap	Mirror / Snap	Backup to disk	Backup to tape

Tier 1 and 2

RTO - **< 4 hrs (Tier 1) and 5 – 24 hrs (Tier 2)**
RPO – the length of time between the last data update and the disaster declaration is from **several minutes to 4 Hours** for SAN attached storage and **24 hours for direct attached**.

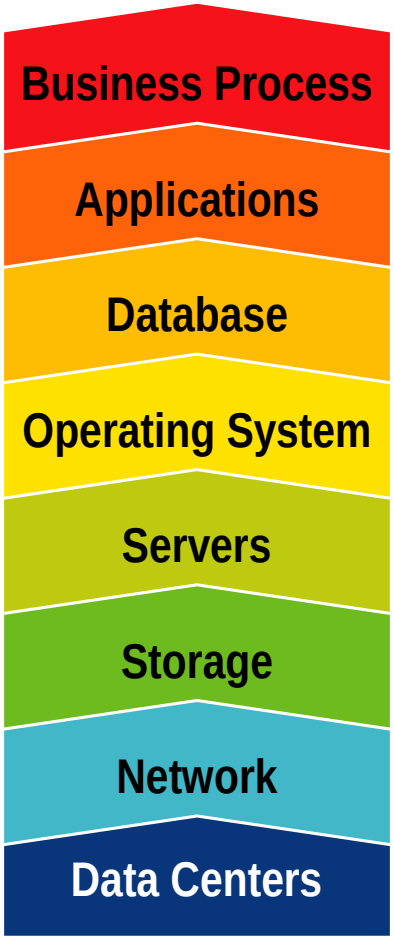
Data Replication <=4hrs

Failover: **Complete failover** from the production site to the DR site

DR Site Architecture: The **DR Site infrastructure will have available** the servers, in either physical or virtual configuration, defined to support agency operations.

Server configuration: **Allocated Servers Physical / Virtual** will already be racked and installed with the respective operating system and application, ready to initialize when the data Logical Unit is connected. **Active/Active – Active/Passive Clustering / SAN storage**

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover



Data Protection: Application data available at the Production SAN storage will be replicated to the DR SAN storage using **asynchronous remote replication capabilities (Raid 10 / Parity Raid)**

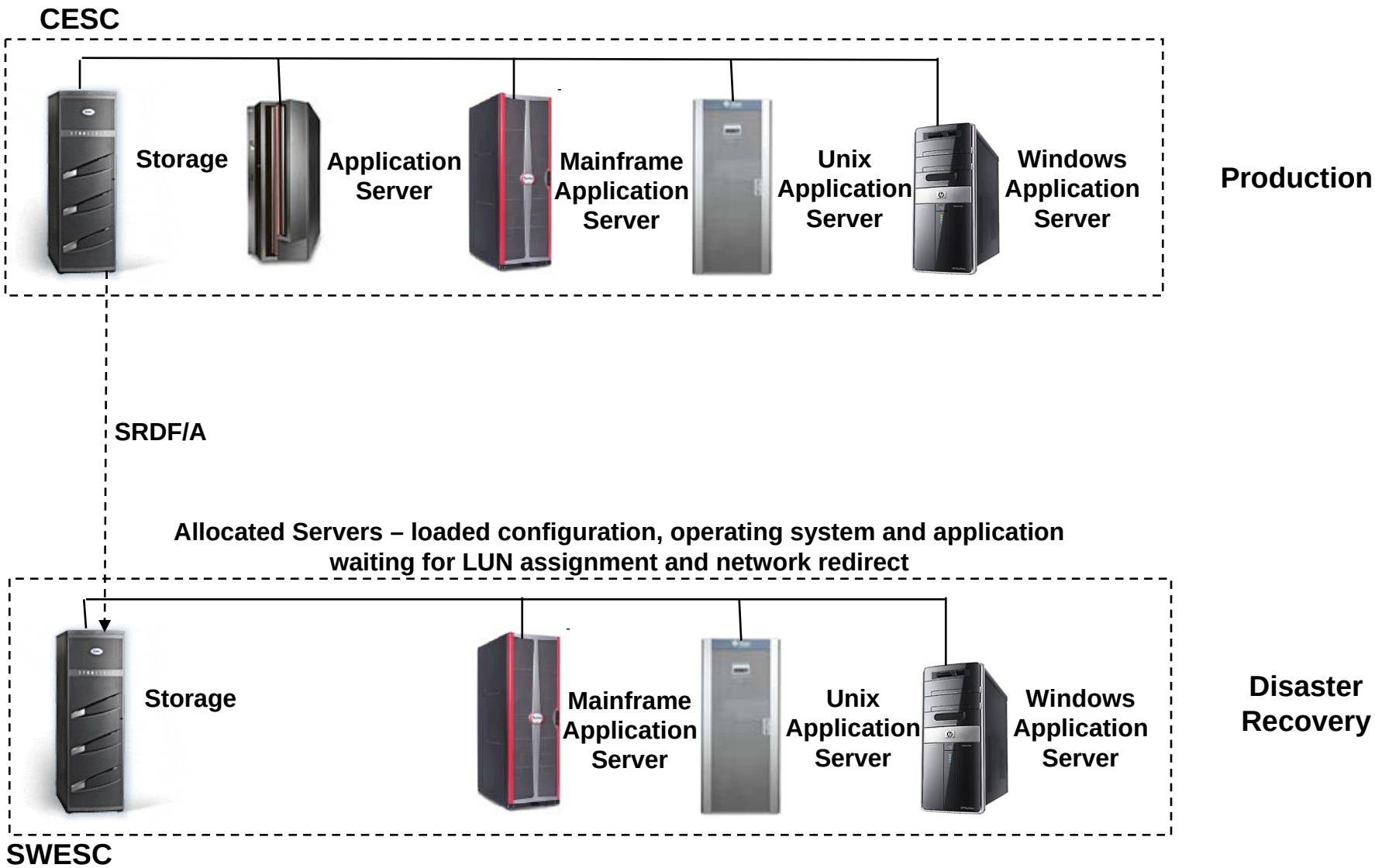
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site; servers may be on a high availability cluster configuration if required

Server Operational Recovery: **High-Availability / Rebuild**

Storage Recovery: SAN The storage array will be replicated to the DR site using an **array based asynchronous replication**. For Tier 2 depending on the application structure, it will be required that data is recovered using a mixed recovery solution.

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed RTO of < 4hrs (Tier 1) / 5-24 hrs (Tier 2)



Tier 3

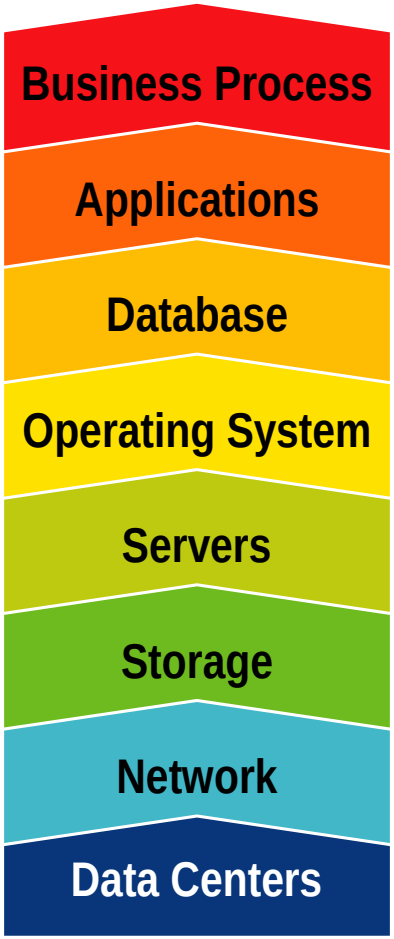
RTO – **25 – 48 hrs**
RPO – the length of time between the last data update and the disaster declaration is from **<=24 hrs.**

Failover: When the operating system and application environments are available and operational and the logical unit with the data is linked to the server a network reconfiguration will enable the complete failover from the production site to the DR site

DR Site Architecture: **Repurposed / Allocated** Servers – connected to SAN Storage.

Server configuration: **Physical / Virtual** will already be racked and **connected to the DR SAN storage**
Active/Active – Active/Passive Clustering

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover



Data Protection: **(Raid 10) / Backup is disk based.** The backup to VTL process will need to be done at a synchronized time to avoid data corruption and all files will be backed up including database, journaled transactions and log files.

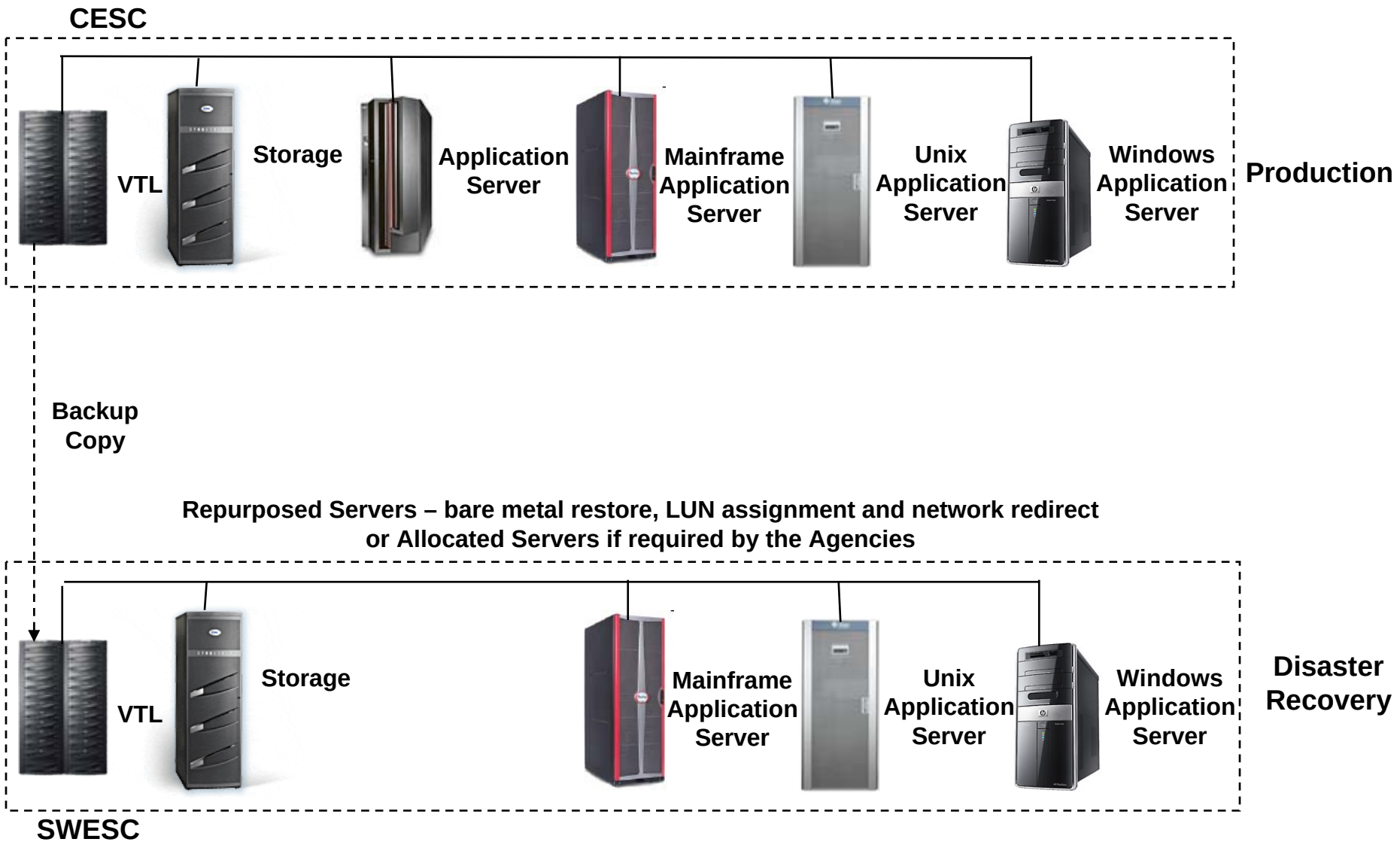
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site

Server Operational Recovery: **Rebuild** The environment is comprised of physical and virtual servers and connected to the DR SAN

Storage Recovery: SAN The storage array will be restored at the DR site using a backup restoration from Virtual Tape Library (VTL). Backup files will be sent from the Production site to the DR site daily through the network, providing an RPO of 24 hours

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed Tier 3



Tier 4, 5, 6

RTO – **49-72 hrs (Tier 4) / > 73 hrs (Tier 5) / with 168 hrs (Tier 6)**

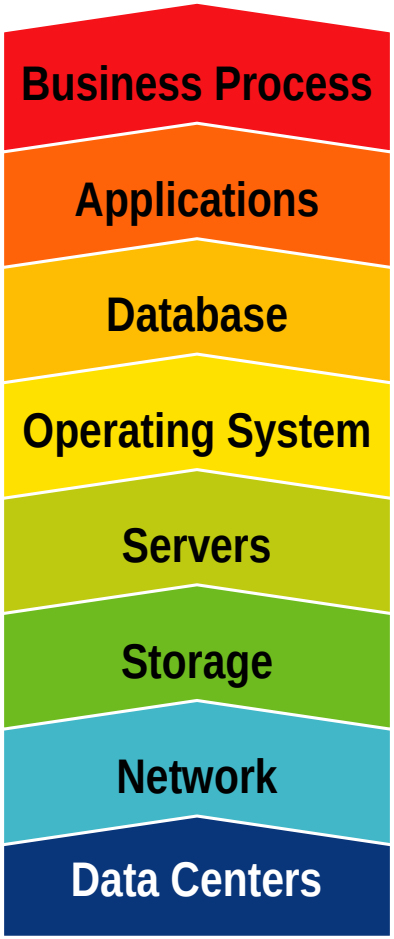
RPO – length of time between the last data update and the disaster declaration is **<=24 Hours**.

Failover: When the operating system and application environments are available and operational and the logical unit with the data is linked to the server a network reconfiguration will enable the complete failover from the production site to the DR site

DR Site Architecture: **Drop Ship / Repurposed / Allocated** connected to SAN / DAS / LOCAL Storage.

Server configuration: Physical/Virtual servers and connected to the DR SAN or through direct attached storage.

Network Recovery: All required network interfaces meeting defined capacity are in place in each data center for site failover



Data Protection: Synchronized-timed backup with restore from Tape. Weekly full copies, daily incremental. **Backup is tape-based** / ***optional RAID 10.***

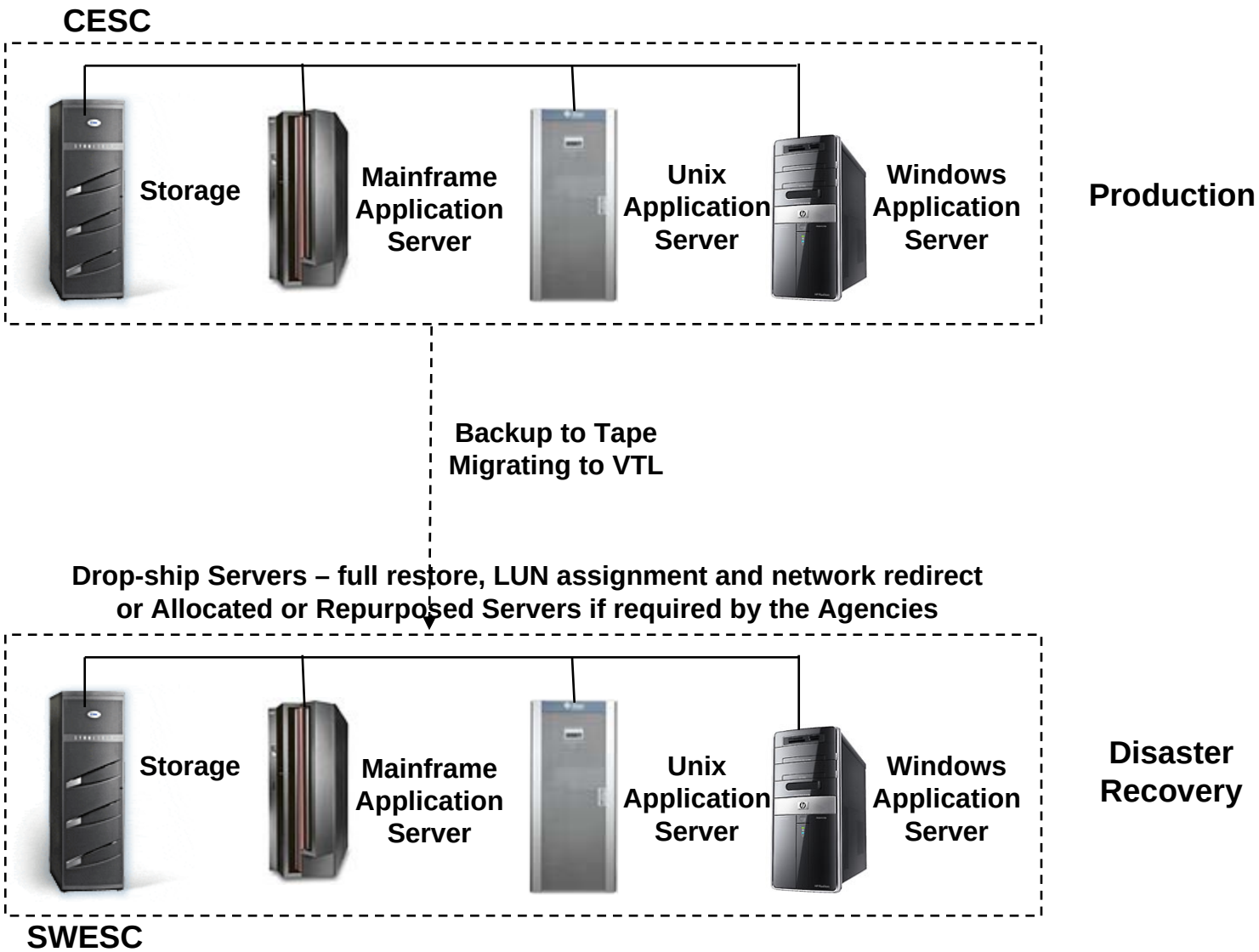
Database Recovery: Database servers will be recovered to physical or virtual server in the failover site.

Server Operational Recovery: **Rebuild** Servers are racked and ready for booting or repurposed or in drop-ship model. Operating system boot images and applications are pre-loaded or readily available or it uses resources like bare metal restore.

Storage Recovery: SAN / DAS / LOCAL The storage array will be restored at the DR site using a backup restoration from magnetic tape.

Infrastructure Recovery: All preventative controls (power, cooling and space requirements) are managed and provided with the service.

Proposed Tier 4, 5, 6



Disaster Recovery Requirement Questionnaire

- Recovery Time Objective / Recovery Point Objective
- Application(s)
- Network
- Infrastructure Components
- Backup
- Data Storage
- Security
- User Testing
- Inter-Dependencies to/with other agencies

Checklist of Results

DISASTER RECOVERY REQUIREMENTS QUESTIONNAIRE

This checklist is for the gathering of Agency DR requirements.

Agency Name:

Date Checklist Completed:

		Data Supplied			
Item	**Application**	**Yes**	**No**	**N/A**	**Comments**
1	Application Software Name				
2	Application type (File System, Online Transaction Processing, Data Warehouse, Web Host, etc.				
3	Application Functional Description				
4	Application Inputs and Outputs				
5	Is there an existing DR Plan/COOP for the application?				
6	Is an offsite disaster recovery facility used? If yes, type of site (hot site, warm site, cold site)				
7	Who provides the offsite disaster recovery facility? (In-house, VITA/NG)				
8	Users (who, number of users, location, expected growth, and benefits)				
9	Percentage of successful recoveries in test and real disaster.				
10	When does the application need to be available for use (24x7x365, Mon-Fri @ 9:00 - 5:00, etc)?				
11	When is the application maintenance window?				
12	What is the guaranteed availability rate of the application (99.999%, 99.99%, 99.9%, 98% etc.)				

Determine Final Recommendations

***Risk Based* Decision Matrix**	Meets RTO, RPO's	Transactional Consistency	Technology Scalability	Technology Maturity	Customer Install Base	Certified Vendor Interoperability	Logical Coruption Protection	Physical Corruption Protection
Tier 1	✓	✓	✓	✓	✓	✓	✓	X
Tier 2	X	X	✓	✓	✓	✓	✓	✓
Tier 3								

***Functionality Based* Decision Matrix**	Enables Offline Backups	Recovery to Granular Point-in-time for App Data	Management & Maintenace Requirements	Granular Recovery from DB Corruption	Protection from Lost Trans in DB Corruption	Easiest to add/modify at later date
Tier 1	✓	X	✓	✓	X	✓
Tier 2	✓	X	X	✓	X	✓
Tier 3	✓	✓	✓	✓	✓	X

Identify Tier-Level Solution

Agency	Application	IPlatform	Status	RTO	RPO	Tier-Level
CWA	EMS	IBM	Non-critical moving to Windows in 2 years	24 hours	72 hours	3
CWA	HTRIS	IBM	Non-critical moving to Windows in 2 years	24 hours	72 hours	3
CWA	File Server	Windows	Business Critical	72 hours	72 hours	3
CWA	Web Server	Windows	Business Critical	24 hours	>4 hours	1

Value Added Services

DR Services

- Assist agencies with IT DR Plan updates or creation
- Assist agencies with identifying business requirements for DR testing
- Assist agencies with identifying business requirements for a DR solution

Testing Services

- Annual test for each agency
- Internal tests performed
  - will uncover and reduce errors
  - speed up recovery process by 'practicing'

Dedicated Services

- Ensure data availability and integrity
- 24/7 availability monitoring
- Real-time performance reporting
- Provides complete activation of processes and procedures at the time of a declared event
- Provides constant monitoring and management of the replication environment
- End-user recovery assistance
- Dedicated team of technical engineers

Virginia Information Technologies Agency

The Center for Internet Security

Cathie Brown, CISSP, CISM

Deputy Chief Information Security Officer

What is CIS?

- Formed in October 2000
- A not-for-profit consortium of *users,* security consultants, and vendors of security software (CIS Members)
- Facilitates teams that develop consensus benchmarks for system & network security configuration
- Facilitates teams that develop consensus security metrics for benchmarking.
- Develops & Distributes the CIS Configuration Assessment Tool (CIS-CAT) to its members.

The Center for Internet Security

- Develops the Configuration Benchmarks
- Develops Audit Tool software that enables users to compare the configuration of their systems to the Benchmarks
- The Benchmarks are distributed free of charge to users (in .pdf format) to propagate their use/adoption worldwide

(**CIS Members receive rights, benefits & resources not available to other users**)

- Commonwealth of Virginia membership covers all COV State Agencies/Institutions (not local govt.)

The Consensus Benchmarks Are:

- Recommended technical control rules/values for hardening OSs, applications, and network devices.
- Downloaded over 1,000,000 times per year.
- Distributed by CIS in .pdf to the general public & machine- readable XML (XCCDF) format to members.
- Used by thousands of organizations worldwide as the basis for their security configuration policies and the standard against which to compare them.

The Security Value of Consensus Benchmarks

The Problem:

The vast majority of cyber attacks exploit known software flaws for which a patch or security configuration control is known.

The Solution:

Research & case studies show that 80-95% of known attempted exploits of vulnerabilities are blocked by the technical security controls & actions recommended in the consensus benchmarks.

The Compliance Value of Consensus Benchmarks

The Problem:

Regulatory requirements for information security are burgeoning. Some explicitly require adoption of configuration best practices (FISMA, PCI), others do so implicitly (ISO, SOX, etc.).

The Solution:

The benchmarks distributed by CIS are the ONLY consensus best practice standards for security configuration both developed and accepted by business/industry and government internationally.

40 Benchmarks are Now Available

- Twenty are for operating systems
- Sixteen are for middleware & applications
- Four are for network devices

13 of the 40 are Available To Members Only

- Machine-Readable XML (XCCDF) Format for use with CIS-CAT & tools that members develop

- The XML benchmarks are available on the CIS Members Web Site at: **http://members.cisecurity.org**

CIS Membership Benefits

1. The right to distribute the benchmarks & tools within your organization.

2. Access to Benchmark Audit Tools with specialized features available only to members.

3. Access to the CIS Members Web Site, including:
   a. Discussion forums;
   b. User groups;
   c. Development versions of new Benchmarks and Audit Tools; and
   d. Resources / download files not available the general user community.

4. Timely electronic notification of updates to the Benchmarks & Audit Tools.

CIS Membership Benefits

5. Enhanced Benchmark and Audit Tool support from CIS staff and developers.

6. An active role in the benchmark consensus process, participating with security specialists from organizations around the world in the definition of best practice standards for security configuration;

7. Visibility for your organization's tangible commitment to Internet security through its inclusion in the Roster of Members on the CIS website and promotional materials;

8. The right to use the CIS Membership Mark on your organization's website and documents, establishing its status as a leader formulating better security standards for systems connected to the Internet.

Register

- Register at http://members.cisecurity.org

More Information Coming Soon

- CIS Representatives will present at an upcoming ISOAG meeting

www.CISecurity.org

Virginia Information Technologies Agency

Network Security at Home Defending the Castle

Bob Baskette, CISSP, CCNP

Security Incident Management Engineer

Defense in Depth – The need

- A home computer system has an inherent value to both the computer system owner & those malicious individuals who seek the data stored on the computer systems & the available processing power the computer systems possess.
- Malicious individuals may be interested in taking over the system to store illegal materials or launch attacks that will be traced back to the compromised system instead of the malicious individual.
- It is the responsibility of the system owner to protect the home network & the systems attached to that network.

Defense in Depth – The Issues

- Studies have shown that a non-patched Microsoft Windows 2000/XP system connected to the Internet can be compromised in as little a 5-minutes.
- A compromised home computer system can send 200,000 spam emails an hour.
- Details on new vulnerabilities are published on an hourly basis.
- Software publishers require time to provide software updates.

Defense in Depth – The Golden Age

- Defense in Depth concepts have not changed in over 1,000 years!
- Confront the attacking force with as many overlapping obstacles as possible to discourage the attack or at least delay the attacking force until response measures can be deployed.
- Castle defenses started with the use of the natural terrain
    - Moat
    - High-wall Outer-Shell
    - Sentries
    - Building walls with windows only above the second floor.

Defense in Depth – Modern Approach

- Firewalls
- Network Address Translation (NAT)
- Wi-Fi Security
- Operating System Hardening
- Email Security
- Anti-Virus / Anti-Spam / Anti-Spyware Software
- Secure Browsers
- Social Networks & On-line Services
- Virtualization

Firewall Information

- Firewalls are hardware devices or software programs that can be configured to filter both inbound & outbound traffic between the home network & the public Internet.
- Firewalls add a layer of protection by blocking unauthorized & potentially dangerous traffic from entering the home network. Firewalls are essential for home networks that have an “always on” connection to the Internet.

Firewall Information

- The selection of a firewall is dependent upon the sensitivity of the computer systems and data to be protected. The value of the assets, the complexity of the computers or networks, & the usage of the Internet will dictate the type & size of firewall that should be used.
- A software-based firewall can be deployed in those cases where the computer system is used simply to access websites & send emails.
- A hardware-based firewall would be more appropriate for those computer systems used for on-line banking, on-line bill paying, on-line shopping, or file hosting services.
- A software-based firewall can be used in combination with a hardware-based firewall to implement the "Defense-in-Depth" best practice, thereby providing multiple layers of traffic filtering.

Basic Firewall Configuration

- Implement a "Client-Only" or "Established/Related" traffic filtering list.
    - Allow only the inbound network traffic that is needed.
    - Define the programs, protocols and ports that should have access to the home network.
    - Block unsolicited traffic from connecting to the home network.
    - Prevent LAN traffic from leaving the home network .
    - Filter all inbound traffic with a source IP-address in the RFC-1918 Private IP-address range.
    - Filter all inbound traffic with a source IP-address that matches the IP-address range used on the home network.
- Enable the "automatic update" feature if one exists for the firewall.
- Periodically check the firewall vendor's website for the latest software updates.

Basic Firewall Configuration (cont'd)

- Change the default "administrator" account & password.
- Disable the remote management option.
- Firewalls should be configured to log activity. These logs should be reviewed AT LEAST once a month to identify any anomalous or unexpected activity.

Additional Firewall Information

- Stateful Packet Inspection (SPI) technology will examine traffic destined for the home network to determine if the inbound traffic is arriving in response to an authorized request.
- MAC address filtering should be employed to prevent rogue devices from connecting to the home network.
- Administrative functions should be limited/assigned to a specific computer system IP-address on the home network.
- If the firewall administrative interface is web-based, only enable the SSL/TCP-port 443 option. Disable the HTTP/TCP-port 80 option.

Additional Firewall Information

- If the firewall administrative interface is text-based, only enable the SSH/TCP-port 22 option. Disable the Telnet/TCP-port 23 option.
  - PuTTY is a SSH program for Microsoft Windows.

- Firewalls should be used in concert with Network Address Translation, operating system hardening, anti-virus, anti-spyware, and anti-spam software as part of a "Defense-in-Depth" strategy for protecting the computer systems attached to the home network from various forms of remote attacks by malicious individuals who want to steal personal information or use the computer systems for illegal activities.

Network Address Translation

- Most hardware-based firewalls and wireless access points provide Network or Port Address Translation.
- NAT/PAT will obfuscate the home network's actual IP-address space.
- NAT/PAT will allow every computer system on the home network to appear as the same IP-address to the Internet so a malicious individual cannot easily determine the actual number of computer systems attached to the home network or which system is utilizing a specific service.

Network Address Translation

- Be default, most home networking NAT/PAT devices will use the 192.168.0.0/24 IP-address range for the home network. This IP-address range should be changed to another private IP-address range defined in RFC-1918.
- Available RFC-1918 IP-address ranges include:
  - 10.0.0.0/8
  - 172.16.0.0/16 – 172.31.0.0/16
- Change the administrative interface on all home routers/firewalls/wireless access points to use something other than 192.168.0.1 or 192.168.0.100. These two IP-addresses are default on most consumer-grade equipment.

Wi-Fi Security

- Physical lay-out
  - Place the wireless access point at center of the home.
  - Limit broadcast distance
- Wireless access point configuration
  - Operate in the 802.11n range if possible.
    - Most current equipment operates at 802.11b or 802.11g.
  - Change the SSID (Service Set Identifier) from the default vendor value.
  - Disable the SSID broadcast if possible.
  - Enable MAC-address filtering.
  - Include all Ethernet and wireless MAC-addresses on the home network in the filter list.
  - Enable Wi-Fi Protection
    - WPA-2 Personal security provides the best protection for a home network
    - WPA security provides adequate protection for a home network
    - WEP has been compromised, but is still better than clear text

Wi-Fi Security

- Disable "Bridge" mode on the wireless access point if only one wireless access point will be installed on the home network.
- Configure the computer systems on the home network that use a wireless connection to operate in an "Infrastructure Mode" only.
  - Wireless "Ad-Hoc" mode will allow a direct connection between two computers using wireless network adapters.
  - Microsoft Windows 2000/XP will bridge an active wireless connection to the wired network in certain network configurations.
  - An "Ad-Hoc" connection to a computer system on the home network will allow a malicious individual to "by-pass" all security measures & connect to the home network.

Operating System Hardening

- Every modern Operating System has vulnerabilities and available exploits with which to attack those vulnerabilities.
- To protect the Operating System:
  - Enable the "Automatic Software Update" feature.
  - Remove software that is no longer needed.
  - Remove trial software once the trial has ended.
  - Do not install unsolicited software from any source.
- Remember, Free Software can be Very Expensive.

Operating System Hardening

- Turn off File Sharing, Print Sharing, NetBios or other services that are not needed.
- Employ the Least Privilege concept
    - Create a separate account for system administration on the computer system.
    - Do not use the name Admin, Superuser, Root, or any other term that would suggest that the account is the Administrator account. The "Administrative" account should only be used to install software & make system modifications.
- Create separate accounts for each user on the computer system. The user accounts should be used for the day to day activities. Limiting access to the system privileges associated with the Administrator account will prevent some of the malicious content spreading across the Internet from getting installed on the computer system.

Operating System – Password Selection

- Ensure that each account on the computer system uses strong passwords.
  - Do not use anything that can be associated with the user such as name, birth date, family member/pet name, or words found in the dictionary.
  - Use phrases or build a password by pulling out the first and last letter of every word of a phrase and use that as the password.
  - Replace characters with numbers such as the '0' (zero) instead of the 'O', 'i' instead of a '1', '3' instead of an 'e', or '4' instead of an 'a'.
  - Do not use the same password on every site.
- To verify the strength of a password, visit the Microsoft password checking site:
  http://www.microsoft.com/protect/yourself/password/checker.mspx

Email Security

- Email Security Best Practices
  - To mitigate the potential threat presented by a spam or phishing email campaign, never open attachments or click links contained in unsolicited email messages.
  - If possible, check with the person who supposedly sent the email to make sure that it is legitimate prior to opening any attachments.
  - Scan any attachments with anti-virus software before opening the attachment.
  - Do not reveal personal or financial information in an email, & do not respond to email solicitations for this information.

Email Security

- Email Security Best Practices
  - Always examine the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain extension such as .com vs. .net.
  - If the legitimacy of an email request needs to be verified, try to verify the origin of the email by contacting the company directly. Never use the contact information provided on a web site connected directly to the email request.
  - An additional step to help mitigate the risk of a phishing campaign is to limit the administrative rights of the local users through the implementation of the Least-Privileged best practice.

Email Security – Additional Steps

- Disable automatic image loading.
- Configure the email client software to send & display email in text format. This will prevent the embedded links in the email from being clickable & will prevent malicious code hidden in the email from running when the email is opened.
- Establish an unique domain name for email accounts. Domains can be registered with companies such as:
  - Network Solutions http://www.networksolutions.com
  - Verisign http://www.verisign.com
  - GoDaddy http://www.godaddy.com
- Create a separate email account for website forms and contact lists.

Anti-X software

- Every computer system on the home network needs an up-to-date version of anti-virus, anti-spyware, anti-spam, and anti-phishing software.
- The leading vendors for Anti-X software are:
  - Norton (Symantec)
  - McAfee
  - Trend Micro
  - Zone Alarm (CheckPoint)
  - Each of these vendors provide a complete software solution for Anti-X and firewall functions.
- Configure the Anti-X software to check for product updates on a daily basis.
- Configure the Anti-X software to scan the entire contents of the hard drive at least once a week.
- Configure the Anti-X software to scan ALL removable media each time the removable media is attached to the computer system.
- Scan ALL installation CD/DVDs for malicious code prior to installing the software.
- Please renew the software update license each year or purchase a new copy of the software at the end of each year. Do not let the Anti-X software expire.

Anti-X Notes

- USB storage devices such memory cards (for digital cameras or MP3 players), flash drive/thumb drives, removable hard drives or digital photo frames are formatted at the factory to simplify installation. During the past three years, these devices have been shipping with additional features such as viruses, trojans, and key logging programs.
    - 500Gbyte and 1Tbyte hard drives purchased by the Federal Government contained a trojan.
    - Digital photo frames sold by Best Buy and CompUSA contained a key logging program.
- Before any USB device is used for the first time:
    - Turn off the Operating System Autorun feature.
    - Scan the device for malicious software.
    - Format memory cards using the built-in digital camera function.
    - Format (zero the drive) new USB hard drives.
- Monitor the computer system:
    - Monitor hard disk space to determine if the available space decreases for an unknown reason – This may indicate a backdoor has been installed on the computer system and the system is storing information for a malicious individual.
    - Monitor the log files and Event Viewer logs for unexpected error messages
- Avoid P2P programs. Multimedia download services such as Limewire, Bearshare, Gnutella and Kazaa can expose the computer system to massive exploits.

Secure Web Browser Information

- Modern-day Browsers
  - Microsoft Internet Explorer 7
  - Mozilla Firefox 3
  - Opera
  - Safari 3
- Browser configuration
  - Disable Active-X controls and applets if possible.
  - Disable the Adobe Flash plug-in if possible.
  - Disable form auto-fill functions.
  - Disable password caching.
  - Install security plug-ins from the software vendor's website to improve the security inspection of the displayed website.
  - Configure the browser to clear all browser information when the browser window is closed.
  - Only accept cookies from the sites that you visit.

Secure Web Browser Information

- Avoid Tab browsing when sending sensitive information.
- Prior to initiating a secure connection to a website where confidential information will be sent to or received from the web server:
  - Close all browser windows.
  - Clear the browser cache.
  - Clear all browser cookies.
- Enable private browsing if supported by your browser.
- Do not ignore SSL certificate warnings.

Secure Web Browsing Concerns

- Take care when surfing the Internet. Even trusted websites can become compromised with code that will redirect your browser to malicious websites or attempt to download malicious code to the computer.
- Beware of the "Pop-Up" window. Never install a program just because a "Pop-Up" window appears with message indicating that a software update or applet is needed. Remember, if a trusted website prompts to install a program, err on the side of caution and say no. Contact the company by telephone and confirm the software update.
    - A popular exploit mechanism is to use an Anti-Virus "Pop-Up" window informing the user of a potential infection on the computer system and to install "Anti Virus Software" to remove the infection. This exploit will either install a program that does nothing but prompt the user for money to remove the "infection" or will attempt to ransom the contents of the computer system. Either way, clicking "Yes" to remove the "infection" actually results in the installation of malicious software.

Secure Web Browsing Password Security

- Use strong passwords for any websites requiring a login.
- Use unique passwords for all websites. Avoid using the same password for similar websites.
- Carefully consider the questions used by a website for automated password resets. Most websites use the same set of common questions for password reset. Most of the answers to these questions can be found in public records or on-line.
    - Place of birth, mother's maiden name, and school information are available in public records.
    - Friends, color preference, hobbies, and pet information often found on Social Network sites.
    - Make of first car can be guessed based on purchasing trends.
- Consider using the option to create your own question/answer combination if possible.

Social Networks & On-line Services

- Social Networks such as MySpace & FaceBook are designed to be online communities focused on interaction betweens friends, families, & others who may share similar interests.
- Social Networks provide a mechanism to allow people to communicate using the means that best suite their lifestyle including email, instant messaging, forums, and blogs.
- Social Networks can increase the risk of Identity Theft & CyberBullying due to their open nature & anonymity granted to its users.

Social Networks & On-line Services Risk Mitigation

Mitigating the potential risks associated with Social Networks.

- Select your screen name carefully – do not include any information such as your name, age, sex, city, or employer.
- Never post anything you would not want to have distributed publicly.
- Never post personally identifying information such as: SSN, first and last name, address, driver's license, telephone number and e-mail address.
- Be careful posting any pictures; they can be altered & re-posted anywhere on the Internet.
- When establishing your account, adjust your profile until you are comfortable with the amount of protection provided to maximize your security.

Virtualization Information

- Virtualization is a mechanism to run multiple instances of an operating system on the same computer.
- Virtualization can also be used to allow different operating systems to run at the same time on the same computer system.
- Popular Virtualization software products include:
  - VMware Workstation for Microsoft Windows and Linux
  - VMware Player for Microsoft Windows and Linux
  - Parallels Workstation for Microsoft Windows and Linux
  - Parallels Desktop for Mac
  - VMware Fusion for Mac

Virtualization Techniques

- Virtualization can be used to fortify the computer system when accessing external resources through the use of "Snapshot" images.
- "Snapshot" images allow the virtual system to be reset to a pre-determined point, removing any changes to the virtual system that have been made since the last snapshot. Reverting to a previous "Snapshot" would remove any malicious code installed within that virtual system while browsing the Internet from that virtual system.
- Virtual systems can be installed to provide specific functions such as:
    - General Internet surfing
    - On-line shopping and on-line banking
    - Email
    - File-sharing and website hosting
- VMware Player is a free software product from VMware. VMware Player can use pre-configured virtual machines from VMware.

Helpful URLs

- To learn more about home network security, please visit the following sites:
  - http://www.securityfocus.com
  - http://www.isc.sans.org
  - http://www.microsoft.com/protect/default.mspx
  - http://www.microsoft.com/security/default.mspx
  - http://www.us-cert.gov
  - http://secunia.com/
  - http://www.cert.org/homeusers/HomeComputerSecurity/
  - http://www.cert.org/tech_tips/home_networks.html

Helpful URLs

- Additional information on firewall configuration can be found at the following URLs:
  - http://www.us-cert.gov/cas/tips/ST04-004.html
  - http://onguardonline.gov/tutorials/firewall-xp-instruct.html
  - http://onguardonline.gov/tutorials/firewall-osx-instruct.html
  - http://www.firewallguide.com

Final Thoughts

- The security of the home network is ultimately decided by how the computer systems are used.
- A "Fully-Patched" computer system is only fortified against known vulnerabilities. "Zero-Day" exploits & unpublished vulnerabilities can still have a negative impact on the computer systems.
- Most home computer systems that become compromised have two components in common:
  - The computer system had outdated anti-virus programs
  - The computer systems were used to download music and movies from the Internet.
- Keep the software on the computer systems up-to-date!
  - Install the latest security updates from the software vendor.
  - Enable Automatic Updates for the operating system, anti-virus, and user applications.
  - Secunia PSI is the FREE security tool that is designed to scan the computer system for installed software and determine if any applications lack security updates. https://psi.secunia.com/

Final Thoughts

- Scan the computer system for malicious software at least once a week.
- Back-up your files on a regular basis.
- Keep all installation CD/DVD media and license keys in a safe place.
- Visit computer security websites to become aware of the current malicious threats.
    - www.isc.sans.org
    - www.us-cert.gov
    - www.securityfocus.com

Questions???

For questions or more information, please contact Commonwealth Security at:

VITASecurityServices@VITA.Virginia.Gov

Thank You!

Virginia Information Technologies Agency

October as Information Security Awareness Month

Nakita Albritton, CISSP, PMP
Information Security Manager/
Continuity of Operations Coordinator

Internet Safety Month

- In 2007, the General Assembly passed House Joint Resolution No. 587 designating September as Internet Safety Month.
  - To promote awareness of the dangers of the Internet & provide information that will assist you & your children in using the Internet safely.

Information Security Month

- Governor Timothy Kaine issued a proclamation designating October as Information Security Awareness Month.
  - To encourage citizens to learn about information security & to put the knowledge to practice.

Governor's Proclamation 2008

Information Security Month Proclamation

- Copy of 2008 Proclamation
  - Available today at the back table. (Please take one per agency or locality)
  - Available online in the VITA Information Security Toolkit.
  - Many thanks to Judy Napier, Deputy Secretary of Technology, for making this happen!

Now Is The Time!

- If you have not begun planning for your Information Security month activities, it is not to late, but time is ticking.

- Start now!

Information Security Month Ideas

- Activities
  - Presentations, Brown Bag Presentations, Demonstrations, Puzzles, Drawings
- Resource Material
  - Brochures, Booklets, Bookmarks, Calendars
- Festive Environment
  - Balloons, Banners, Posters

Resource Materials

- Brochures, Booklets, Bookmarks, Calendars
  - MS-ISAC resource materials are available in the VITA Information Security Toolkit.
  - Department of Motor Vehicles (DMV) has graciously offered to provide printing services.
    - For a price quote, please contact Damian M. McInerney by email at DAMIAN.MCINERNEY@dmv.virginia.gov or by phone at 804-367-0925.

Let Us Hear From You

In early November, please share a brief summary of your Information Security month activities with us by emailing us at VITASecurityServices@Virginia.Gov.

WE ARE LOOKING FORWARD TO HEARING FROM YOU!

Reference

Commonwealth Information Security Toolkit!

http://www.vita.virginia.gov/security/default.aspx?id=5146

Virginia Information Technologies Agency

Commonwealth Security Annual Report

Peggy Ward
Chief Information Security and Internal Audit Officer

§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.

Explanation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

Agency
- Agency Abbreviation

Security Audit Plan Rec'd
- Indicates whether agency has submitted a Security Audit Plan to Commonwealth Security and Risk Management for all systems classified as sensitive based on confidentiality, integrity, or availability.
- Options: Current = Received and up to date, No = Not Received, Outdated = Audit Plan was submitted but requires update, Extension Expired = An Exception was filed but has expired and Audit Plan has not been Received.

ISO Designated
- Indicates whether agency head has designated an Information Security Officer for the agency and provided the person's name, title and contact information to VITA no less than biennially.
- Options: YES/NO

Explanation – Continued

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

Attended IS Orientation (Extra Credit)

- Indicates the number of attendees that an agency has sent to attend Information Security Orientation.
- This data point is an "Extra Credit" data point where as it is not currently a requirement, but attendance is highly encouraged for ISO's and all interested parties.
- Options: 0 - ∞

IT DR Plan Rec'd

- Indicates whether agency has submitted an IT Disaster Recovery Plan.
- Options: YES = Submitted, YES/UPD = Submitted an updated IT DR Plan, NO = Has not submitted IT DR Plan, N/A = Not Applicable (Agency is not a customer of the IT Partnership)

Explanation – Continued

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

CAP's Rec'd

- Indicates whether the agency has submitted Corrective Action Plans (CAP's) for vulnerabilities identified in Security Audits.
- *Note* CAP's are to be submitted to Commonwealth Security and Risk Management one month after the completion of an audit and updates submitted quarterly for open vulnerabilities.
- Options: YES = Agency performed Security Audits and submitted CAP's, NO = Agency's Security Audit Plan indicates Security Audit was scheduled but has not submitted CAP, N/A = Not applicable, either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.

CAP's Status

- Indicates the number of Corrective Action Plans submitted and the number of Security Audits scheduled based on the Security Audit Plan.
- Options: [Numbers of CAP's received] of [number of Security Audits scheduled] (example - 1 of 1, 0 of 1, 1 of 2, etc…), N/A = either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.

Secretariat: Administration

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CHR	NO	YES	0	YES	N/A	N/A
DGS	Current	YES	0	YES	NO	0 of 3
DHRM	Current	YES	0	YES/UPD	N/A	N/A
DMBE	NO	YES	2	YES	N/A	N/A
EDR	Current	YES	3	YES/UPD	N/A	N/A
SCB	Current	NO	1	YES	NO	0 of 6
SBE	Current	NO	1	YES	N/A	N/A

Secretariat: Agriculture & Forestry

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOF	Current	YES	1	YES	N/A	N/A
VADACS	Current	YES	33	YES	YES	1 of 1

Secretariat: Commerce & Trade

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DBA	NO	YES	1	YES	N/A	N/A
BOA	Current	YES	1	YES	NO	0 of 3
DHCD	Current	YES	0	YES	NO	0 of 4
DMME	Current	YES	1	YES	YES	1 of 3
DOLI	NO	YES	3	YES	N/A	N/A
DPOR	Current	YES	1	YES	NO	0 of 5
TIC	NO	NO	0	NA	N/A	N/A
VEC	Current	YES	2	YES/UPD	NO	0 of 6
VEDP	NO	YES	0	YES	N/A	N/A
VHDA	NO	NO	1	NA	N/A	N/A
VNDIA	NO	NO	0	NA	N/A	N/A
VRA	NO	NO	0	NA	N/A	N/A
VRC	EXTENSION EXPIRED	YES	2	YES	N/A	N/A

Secretariat: Education (excluding Higher Ed)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOE	Current	YES	1	YES	NO	0 of 5
FCMV	NO	YES	0	NO	N / A	N / A
GH	NO	YES	0	NO	N / A	N / A
JYF	Current	YES	1	YES	NO	0 of 3
LVA	Current	YES	1	YES	N / A	N / A
SCHEV	EXTENSION EXPIRED	YES	0	YES	N / A	N / A
SMV	NO	YES	0	YES	N / A	N / A
VCA	NO	NO	0	YES	N / A	N / A
VMFA	Current	YES	2	YES	YES	2 of 2

Secretariat: Education (Higher Ed only)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CNU	Current	YES	0	NA	N/A	N/A
GMU	Current	YES	1	NA	YES	11 of 22
JMU	Current	YES	0	NA	YES	3 of 3
LU	Current	YES	1	NA	YES	1 of 2
NSU	NO	YES	2	NA	N/A	N/A
ODU	Current	YES	1	NA	YES	3 of 4
RU	Current	YES	0	NA	N/A	N/A
UMW	Current	YES	1	NA	NO	0 of 1
VCCS	Current	YES	3	NA	YES	1 of 2
VMI	Current	YES	0	NA	N/A	N/A
VSU	Current	YES	3	NA	NO	0 of 10

Secretariat: Finance

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOA	NO	YES	4	YES	N/A	N/A
DPB	Extension Expired	Yes	2	YES/UPD	N/A	N/A
TAX	Current	YES	1	YES	YES	10 of 16
TRS	Current	YES	2	YES	YES	1 of 9

Secretariat: Health & Human Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DHP	Current	YES	0	YES	N/A	N/A
DMAS	Current	YES	6	YES	NO	0 of 5
DMHMRSAS	Current	YES	13	YES	N/A	N/A
DRS	Current	YES	0	YES	NO	0 of 5
DSS	Current	YES	2	YES/UPD	NO	0 of 18
TSF	NO	NO	0	NO	N/A	N/A
VDA	Current	YES	1	YES	N/A	N/A
VDH	Current	YES	3	YES	YES	9 of 11

Secretariat: Natural Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DCR	Current	YES	1	YES	NO	0 of 1
DEQ	Current	YES	4	YES	YES	1 of 1
DGIF	NO	YES	1	YES	N/A	N/A
DHR	Current	YES	2	YES	N/A	N/A
MRC	Current	YES	2	YES/UPD	YES	4 of 4
VMNH	NO	YES	1	YES	N/A	N/A

Secretariat: Public Safety

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
ABC	Current	YES	1	YES	YES	5 of 5
CASC	NO	NO	0	NO	N / A	N / A
DCJS	Current	YES	2	YES	NO	0 of 5
DFP	NO	YES	1	NO	N / A	N / A
DFS	Current	YES	1	N / A	N / A	N / A
DJJ	Current	YES	3	YES	NO	0 of 1
DMA	NO	NO	0	YES	N / A	N / A
DOC	Current	YES	3	YES	NO	0 of 6
DOCE	NO	YES	1	YES	N / A	N / A
DVS	NO	YES	1	YES	N / A	N / A
VDEM	NO	YES	1	YES	N / A	N / A
VSP	Current	YES	3	YES	N / A	N / A

Secretariat: Technology

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CIT	Current	YES	1	YES	NO	0 of 1
VITA	Current	YES	20	YES	N/A	N/A

Secretariat: Transportation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DMV	Current	YES	2	YES	NO	0 of 7
DOAV	NO	YES	2	YES	N / A	N / A
DRPT	Current	YES	1	YES	N / A	N / A
MVDB	NO	YES	0	YES	N / A	N / A
VDOT	Current	YES	5	YES	YES	1 of 3

Independent Branch Agencies

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
IDC	NO	YES	4	N / A	N / A	N / A
SLD	NO	YES	2	N / A	N / A	N / A
SCC	NO	YES	3	N / A	N / A	N / A
VCSP	YES	YES	3	N / A	N / A	N / A
VOPA	NO	NO	0	N / A	N / A	N / A
VRS	NO	YES	2	N / A	N / A	N / A
VWCC	NO	YES	0	N / A	N / A	N / A

Other

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
GOV	Extension Expired	YES	1	YES	N / A	N / A
OAG	NO	YES	1	NA	N / A	N / A

Questions?

Upcoming Events

UPCOMING EVENTS! 9/23

AITR Meeting

Tuesday, September 23th, 8:30 am

UPCOMING EVENTS! 10/6-7

VA SCAN – October 6-7, 2008

The VA SCAN 2008 conference registration is $125; pre-registration is required.

The fee includes the conference program, a Monday evening reception, and lunches and breaks for both days. Special room rates are available at The Inn at Virginia Tech, as well as the Hawthorn Suites.

Registration deadline is September 29, 2008. Register at: http://www.cpe.vt.edu/vascan2008/registration.html

http://www.cpe.vt.edu/vascan2008/index.html

UPCOMING EVENTS! 10/20

Commonwealth Information Security Council Meeting

Monday, October 20th, 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 VITASecurityServices@vita.virginia.gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at: http://www.vita.virginia.gov/security/default.aspx?id=5128

UPCOMING EVENTS! 10/23

NEXT ISOAG MEETING!

October 23rd, 1:00 – 4:00 pm @ CESC

DRAFT Agenda

Playing Safely in the Cloud – Marie Greenberg, SCC

Safely Playing in the Cloud - Steve Werby, VCU

Commonwealth & COV Partnership Security Incident Handling – Michael Watson & Don Kendrick, VITA

UPCOMING EVENTS! 10/27

IS Orientation

Wednesday, October 29th, 1:30 pm to 4:00 pm @ CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email VITASecurityServices@vita.virginia.gov

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!