



# ISOAG Meeting

June 7, 2017

Welcome to CESC



# Welcome and Opening Remarks

Michael Watson

June 7, 2017



# ISOAG June 7, 2017 Agenda

- |                                      |                      |
|--------------------------------------|----------------------|
| I. Welcome & Opening Remarks         | Mike Watson, VITA    |
| II. NIST Policies                    | Kelley Dempsey, NIST |
| III. Raising Cybersecurity Awareness | Ralph Mosios, CISSP  |
| IV. Upcoming Events                  | Mike Watson, VITA    |
| V. Partnership Update                | Northrop Grumman     |

# Information Security Continuous Monitoring for Systems and Organizations

## NIST Special Publication 800-137

Virginia Information Security Officers Advisory Group

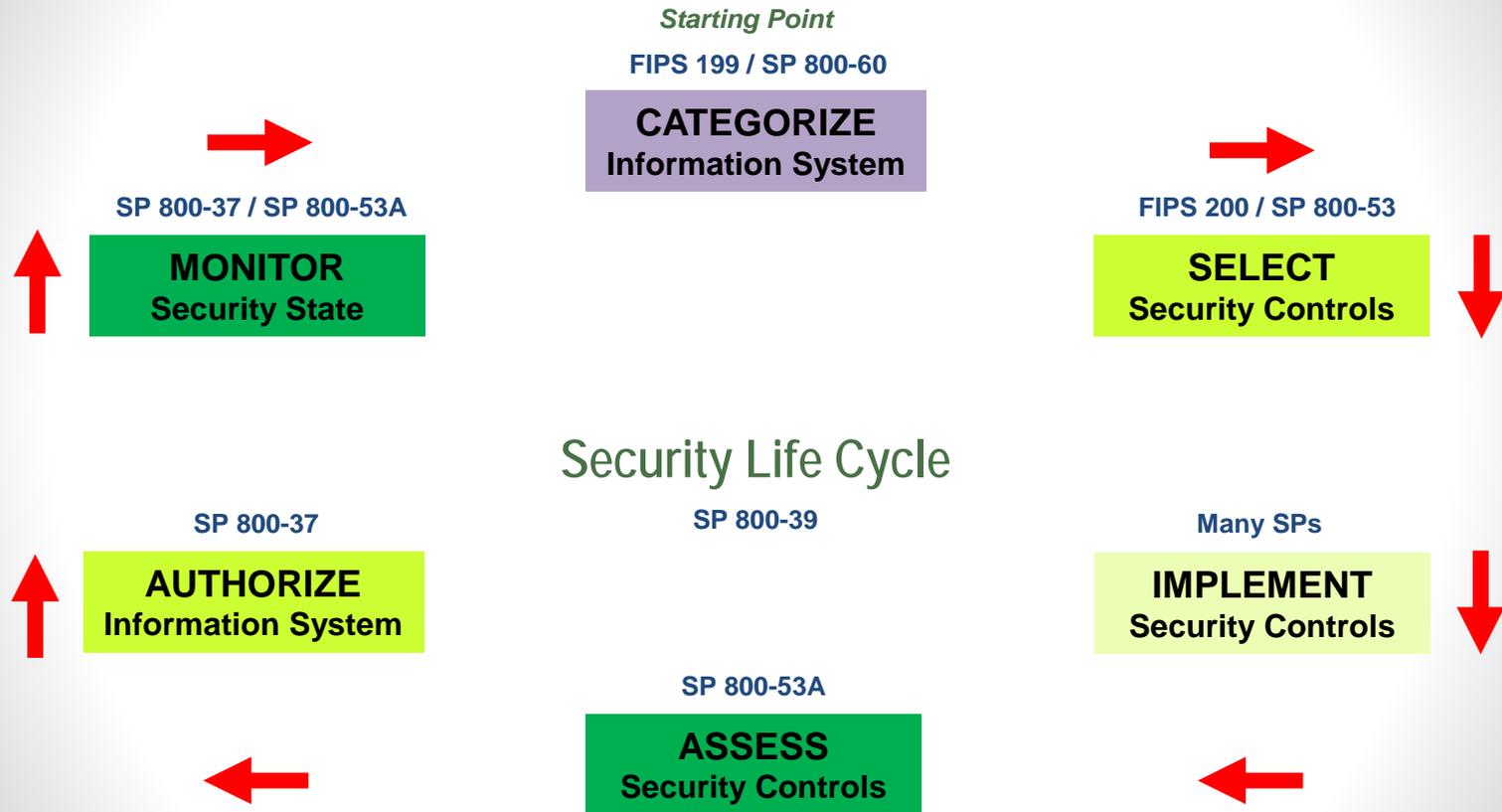
June 7, 2017

Kelley Dempsey

*Computer Security Division  
Information Technology Laboratory*



# Risk Management Framework



# Why Monitor Continuously?

**Continuous Monitoring is the only way to maintain situational awareness of organizational and system security posture in support of risk management.**

# NIST SP 800-137 Definition

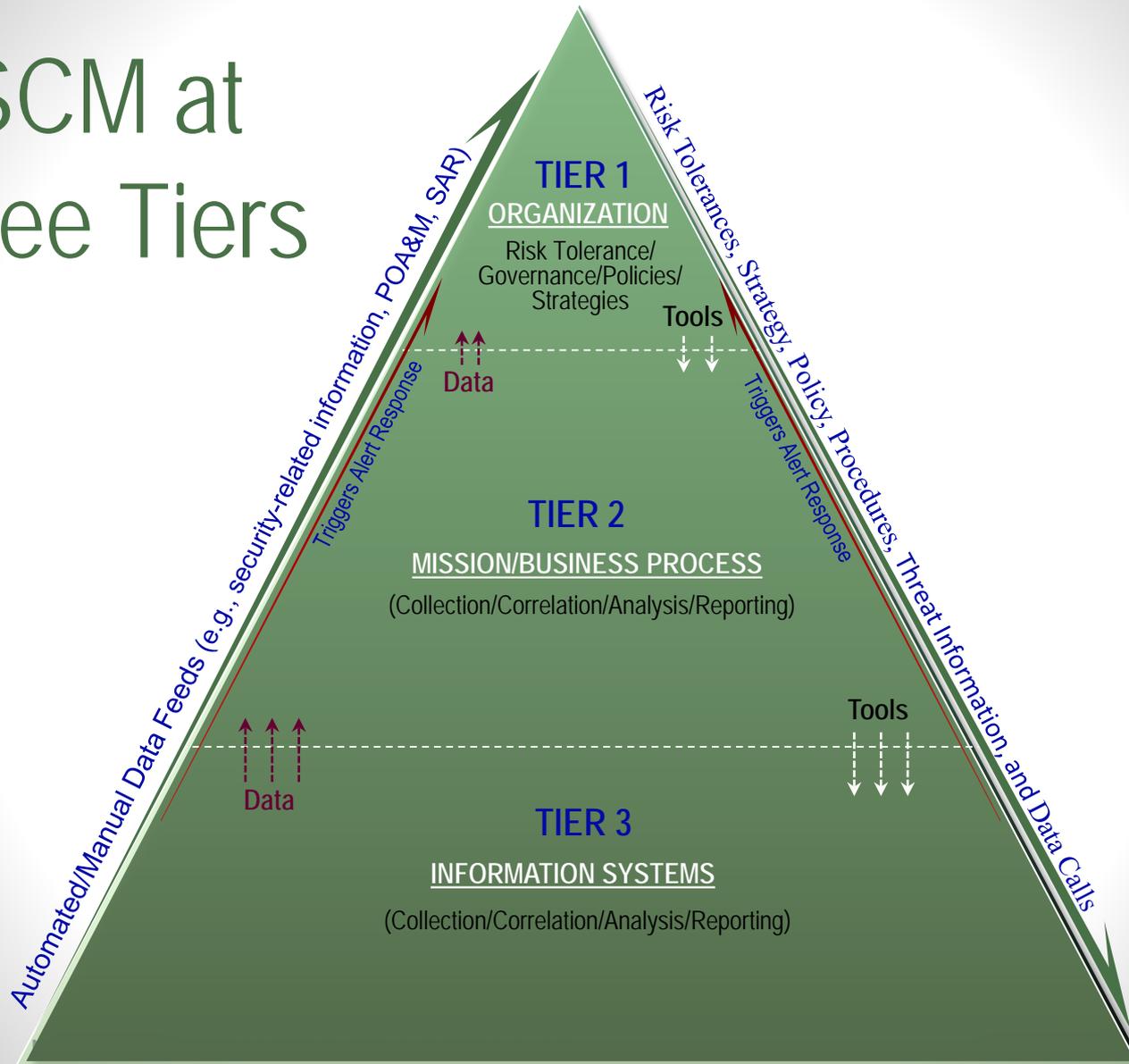
Information security continuous<sup>\*</sup> monitoring (ISCM) is **maintaining ongoing<sup>\*</sup> awareness** of information security, vulnerabilities, and threats to **support organizational risk management decisions**

\* The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals.

# Information Security Continuous Monitoring (ISCM) Objectives

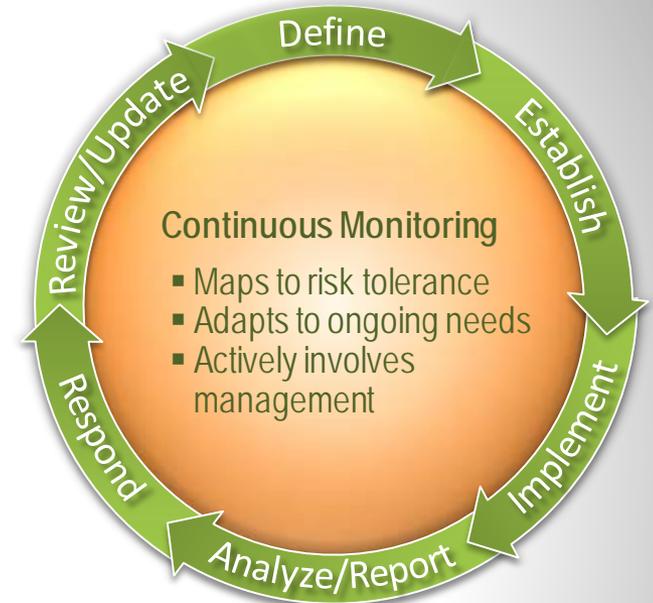
- Conduct ongoing monitoring of security
- Determine if security controls continue to be effective over time
- Respond to risk as situations change
- Ensure monitoring and reporting frequencies remain aligned with organizational threats and risk tolerance

# ISCM at Three Tiers



# ISCM Process Steps

1. **Define** continuous monitoring strategy
2. **Establish** continuous monitoring program
  - a) Determine **metrics**
  - b) Determine monitoring **frequencies**
  - c) Develop ISCM **architecture**
3. **Implement** the monitoring program
4. **Analyze** security-related information (data) and **report** findings
5. **Respond** to findings
6. **Review** and **update** monitoring strategy and program



# Step 1: Define the ISCM Strategy

- Tier 1 - Organization:
  - Define the organization-wide strategy in accordance with organizational risk tolerance (developed at Tier 1 based on guidance in NIST SP 800-39)
  - Develop policies to enforce the strategy
- Tier 2 – Mission/Business Process:
  - Assist/provide input to Tier 1 on strategy and policies
  - Develop procedures/templates to support Tier 1 strategy and fill in gaps
- Tier 3 – Information System:
  - Assist/provide input to Tier 2 on procedures
  - Establish information system-level procedures

# Step 2: Establish the ISCM Program

Three parts:

- a) Determine metrics
- b) Determine monitoring frequencies
- c) Develop technical architecture

## Step 2a: Determine Metrics

- Metrics - **All** the security-related information from assessments and monitoring (manually **and** automatically generated) **organized** into meaningful statistics that support decision making
- Security-related information from multiple sources may support a single metric
- Metrics should **have a meaningful purpose** that is mapped or tied to a specific objective that helps maintain or improve the security posture of the system/organization

## Step 2b: Establish Monitoring and Assessment Frequencies

- Monitor metrics and each control with varying frequencies
- Multiple requirements within a control may have to be monitored with differing/varying frequencies

# Frequency Determination Criteria

- **Control volatility**
- Organizational and system risk tolerance
- Current threat and vulnerability information
- System categorization/impact levels
- Controls with identified weaknesses
- Controls/components providing critical security functions
- Risk assessment results
- Output of monitoring strategy reviews
- Reporting requirements

# Step 2c: Develop ISCM Architecture

- Continuous monitoring architecture uses standard protocols and specifications
- Organizations leverage existing tools, applications, and infrastructure for continuous monitoring architecture
- NISTIRs 7756, 7799, & 7800 describe a technical architecture that support ISCM (CAESARS)
- NISTIR 8011 describes a monitoring methodology and specific defect checks - use automated tools to compare desired state to actual state

# Step 3: Implement the ISCM Program

- **All** controls and metrics are monitored and/or assessed (common, system, and hybrid controls) at the frequency identified in step three
- Tier 2 - Implement tools and processes associated with common controls and organization-wide monitoring (IDPS, vulnerability scanning, configuration management, asset management, etc.)
  - Organization-wide monitoring will pull at least some security-related information from the system level
- Tier 3 – Implement tools and processes pushed down from Tier 2 and fill in any gaps at the system level
- Tiers 2 and 3 – Organize/prepare data for analysis

# Step 4: Analyze Data and Report Findings

- Analyze Data in the context of:
  - Stated organizational risk tolerance
  - Potential impact of vulnerabilities on organizational and mission/business processes
  - Potential impact/costs of mitigation options (vs. other response actions)
- Report on Assessments
- Report on Security Status Monitoring

# Step 5: Respond to Findings

- Determine if the organization will:
  - Take remediation action
  - Accept the risk
  - Reject the risk
  - Transfer/Share the risk
- Specific response actions will vary by Tier
- May need to prioritize remediation actions

## Step 6: Review/Update the ISCM Strategy

- Organizations establish a process for reviewing and modifying the strategy
- Various factors may precipitate changes to the strategy

## Step 6: Strategy Review Considerations

- Is the strategy an accurate reflection of organizational risk tolerance?
- Applicability of metrics
- Applicability/appropriateness of:
  - Monitoring frequencies
  - Reporting requirements

## Step 6: Strategy Update Factors

- Changes to missions/business processes
- Changes in enterprise and/or security architecture
- Changes in risk tolerance
- Revised threat or vulnerability information
- Increase or decrease in POA&Ms for specific controls or metrics
- Trend analyses of status reporting output

# ISCM Automation: The Need for Caution

- Automated tools may lead to a false sense of security
  - A complete picture of overall security posture may not be provided
  - May not provide information on nontechnical security controls
  - May not be possible to automate monitoring the effectiveness of policies and procedures
  - May not be able to monitor all assets/all platforms
- The tools must be monitored for accuracy and integrity
- The tools may generate a quantity of data too large for adequate analysis and response
- The tools must be interoperable

# NIST Special Publication 800-171: Protecting CUI in Nonfederal Systems and Organizations

Virginia Information Security Officers Advisory Group

June 7, 2017

*Kelley Dempsey*  
*NIST IT Laboratory*  
*Computer Security Division*

# What is Controlled Unclassified Information?

Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

-- Executive Order 13556

# Controlled Unclassified Information (CUI)

Supports federal missions and business functions that affect the economic and national security interests of the United States.



# Executive Order 13556

## Controlled Unclassified Information

November 4, 2010

- Established a governmentwide Controlled Unclassified Information (CUI) Program to standardize the way the Executive branch handles unclassified information that requires protection.
- Designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the CUI program.

*Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.*

```
#pragma once
MSC_VER > 1000
#endif // _MSC_VER > 1000
#ifndef AFXWIN_H
#error include "afxwin.h" before including this file
#endif
#include "resource.h"
// CDMotionApp
// See DMotion.cpp for the implementation
class CDMotionApp : public CWinApp
{
public:
    CDMotionApp();
// Overrides
// ClassWizard generated virtual function overrides
//{{AFX_VIRTUAL(CDMotionApp)
public:
    virtual BOOL InitInstance();
//{{AFX_VIRTUAL
// Implementation
//{{AFX_MSG(CDMotionApp)
afx_msg void OnAppAbout();
// NOTE - the ClassWizard will add and remove member
// functions here.
#endif
};
```

# The CUI Registry

[www.archives.gov/cui/registry/category-list.html](http://www.archives.gov/cui/registry/category-list.html)

- Online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent.
- Identifies approved CUI categories and subcategories (with descriptions of each) and the basis for controls.
- Sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.



# An urgent need... A national imperative

The protection of **Controlled Unclassified Information** while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can *directly* impact the ability of the federal government to successfully carry out its designated missions and business operations.

-- NIST Special Publication 800-171

# Nonfederal Organization

An entity that owns, operates, or maintains a nonfederal information system.

-- NIST Special Publication 800-171

# Nonfederal Organizations

## *Some Potential Examples*

- Federal contractors
- State, local, and tribal governments
- Colleges and universities



# The Big Picture

A three-part plan for the protection of CUI

- Federal CUI rule (32 CFR Part 2002) establishes the required controls and markings for CUI governmentwide.
- NIST Special Publication 800-171 defines security requirements for protecting CUI in nonfederal information systems and organizations.
- Federal Acquisition Regulation (FAR) clause to apply the requirements of the federal CUI rule and SP 800-171 to nonfederal organizations (planned for 2017).

# Purpose of SP 800-171

Provide requirements for protecting the confidentiality of CUI:

- When the CUI is resident in *nonfederal* information systems and organizations.
- Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.
- When the nonfederal organization is *not* collecting or maintaining information **on behalf of** a federal agency OR using or operating an information system **on behalf of** a federal agency.

# Applicability of SP 800-171

- CUI requirements apply only to components of nonfederal information systems that **process, store, or transmit CUI**, or provide security protection for such components.
- The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

# Three Primary Assumptions

1. Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal information systems or nonfederal information systems.
2. Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal information systems and organizations.
3. The confidentiality impact value for CUI is no lower than *moderate* in accordance with FIPS Publication 199.

# Additional Assumptions

## Nonfederal Organizations: —

- Have information technology infrastructures in place
  - Are not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI
- Have controls in place to protect their information
  - May also be sufficient to satisfy the CUI requirements
- May not have the necessary organizational structure or resources to satisfy every CUI security requirement
  - Can implement alternative, but equally effective, security measures
- Can implement a variety of potential security solutions
  - Directly or through the use of managed services

# CUI Security Requirements

Basic and derived security requirements are obtained from FIPS 200 and NIST SP 800-53 initially — and then *tailored* appropriately to *eliminate* requirements that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government).
- Not directly related to protecting the confidentiality of CUI.
- Expected to be routinely satisfied by nonfederal organizations without specification.



- Access Control.
  - Audit and Accountability.
  - Awareness and Training.
    - Configuration Management.
    - Identification and Authentication.
    - Incident Response.
    - Maintenance.
      - Media Protection.
      - Physical Protection.
    - Personnel Security.
    - Risk Assessment.
    - Security Assessment.
    - System and Communications Protection
  - System and Information Integrity.

# Security Requirements

14 Families

Obtained from FIPS 200 and  
NIST Special Publication 800-53

# Security Requirement

## Configuration Management Example

### Basic Security Requirements (FIPS 200):

- 3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

### Derived Security Requirements (SP 800-53):

- 3.4.3 Track, review, approve/disapprove, and audit changes to information systems.
- 3.4.4 Analyze the security impact of changes prior to implementation.
- 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

# Contact Information

## *Project Leader and NIST Fellow*

Dr. Ron Ross  
(301) 975-5390  
[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

## *Senior Information Security Specialist*

Kelley Dempsey  
(301) 975-2827  
[kelley.dempsey@nist.gov](mailto:kelley.dempsey@nist.gov)

## *Information Security Specialists*

Ned Goren  
(301) 975-5233  
[nedim.goren@nist.gov](mailto:nedim.goren@nist.gov)

Michael Nieves  
(301) 975-2228  
[michael.nieves@nist.gov](mailto:michael.nieves@nist.gov)

Jody Jacobs  
(301) 975-4728  
[jody.Jacobs@nist.gov](mailto:jody.Jacobs@nist.gov)

Comments: [sec-cert@nist.gov](mailto:sec-cert@nist.gov) (goes to all of the above)

Web: [csrc.nist.gov/sec-cert](http://csrc.nist.gov/sec-cert)

## *Administrative Support*

Peggy Himes  
(301) 975-2489  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## *Team Lead and Information Security Specialist*

Victoria Pillitteri  
(301) 975-8542  
[victoria.pillitteri@nist.gov](mailto:victoria.pillitteri@nist.gov)





# **Raising Cybersecurity Awareness at a Small Agency, What Works for Me, Will it Work for You???**

**Ralph Mosios**

**Federal Housing Finance Agency**

**Chief Information Security Officer**

**June 7, 2017**

# AGENDA

- Who is FHFA?
- The FHFA Security Awareness Program – Circa 2011
- Transition to the Human Firewall Campaign
- Cybersecurity Newsletters
- The Threat Landscape
- The Social Engineering Experiment
- Social Engineering Results
- How You Can Be Vigilant
- Final Thoughts...

# WHO IS THE FEDERAL HOUSING FINANCE AGENCY?

- On July 30, 2008, the Housing and Economic Recovery Act of 2008 (HERA) was enacted, creating FHFA with the combined responsibilities of the Office of Federal Housing Enterprise Oversight, the Federal Housing Finance Board and the HUD Government-Sponsored Enterprises mission team. HERA also provided FHFA with additional authority to regulate Fannie Mae, Freddie Mac and the 12 Federal Home Loan Banks.
- These government-sponsored enterprises provide more than \$5.7 trillion in funding for the U.S. mortgage markets and financial institutions.

# FHFA DEMOGRAPHICS

- 548 Federal Employees
- 56% Male/44% Female
- Average Age is 48
- 88.7% of employees have a bachelor's degree or higher (59% have advanced degrees).
- FHFA has the second highest percent of advanced degrees.

# THE FHFA SECURITY AWARENESS PROGRAM – CIRCA 2011

- New users received general awareness training during employee indoctrination.
- 90% of employees received annual security training.
  - Computer-based training was conducted.
- Users required to re-sign annual rules of behavior.
- No real indication of how effective the program was.

# TRANSITION TO THE HUMAN FIREWALL CAMPAIGN

- Distributed monthly cybersecurity newsbytes
  - Non-technical, user friendly articles designed primarily for home use.
- Enhanced Security Intranet site by posting useful links:
  - Fighting Identity Theft - Federal Trade Commission's Consumer Protection Division
  - Consumer and Internet Safety - Federal Trade Commission's Consumer Protection Division
- Educated users to report suspicious email / behavior to the FHFA Help Desk.

# CYBERSECURITY NEWSLETTERS



# FHF A *Intranet*

[Site Map](#) [Contact Us](#)

Search This Site

Cloudy 51° F IT STATUS: **AVAILABLE**

[Ethics](#) [Help Desk](#) [Life Safety & Security](#) [IMS](#) [Risk Reports](#) [Org Charts](#) [Supervision Information](#) [WebTA](#)

[Home](#) • [Office of the Chief Operating Officer](#) • [Office of Technology and Information Management](#) • [Information Technology Security](#) • [Cyber Security Newsbytes/Security Articles](#)

## Cyber Security Newsbytes/Security Articles

Cyber Security Newsbytes/Security Articles

### Cyber Security Newsbytes

+ [2015](#)

- [2014](#)

[Make Your List and Check it Twice: Follow These Tips for Securing Your New Computer or Device - December 2014](#)

[Online Holiday Shopping: Tips for Keeping Your Information Secure - November 2014](#)

[Social Media Scams - Spot Them Beforehand! - October 2014](#)

[Secure Online Banking - September 2014](#)

[How to Recognize Phishing Messages - August 2014](#)

[What Are Bots, Botnets and Zombies? - July 2014](#)

[Hacked? Now What? - April 2014](#)

[Protect Yourself from Online Tax Scams - March 2014](#)

[2014 Cyber Security Outlook - February 2014](#)

[A Few Tips to Protect Yourself When Shopping with Retailers - January 2014](#)

+ [2013](#)

+ [2012](#)

+ [2011](#)

### IT Security Headline News

- <http://www.infosecurity-us.com/>
- <http://searchsecurity.techtarget.com/>



# THE THREAT LANDSCAPE

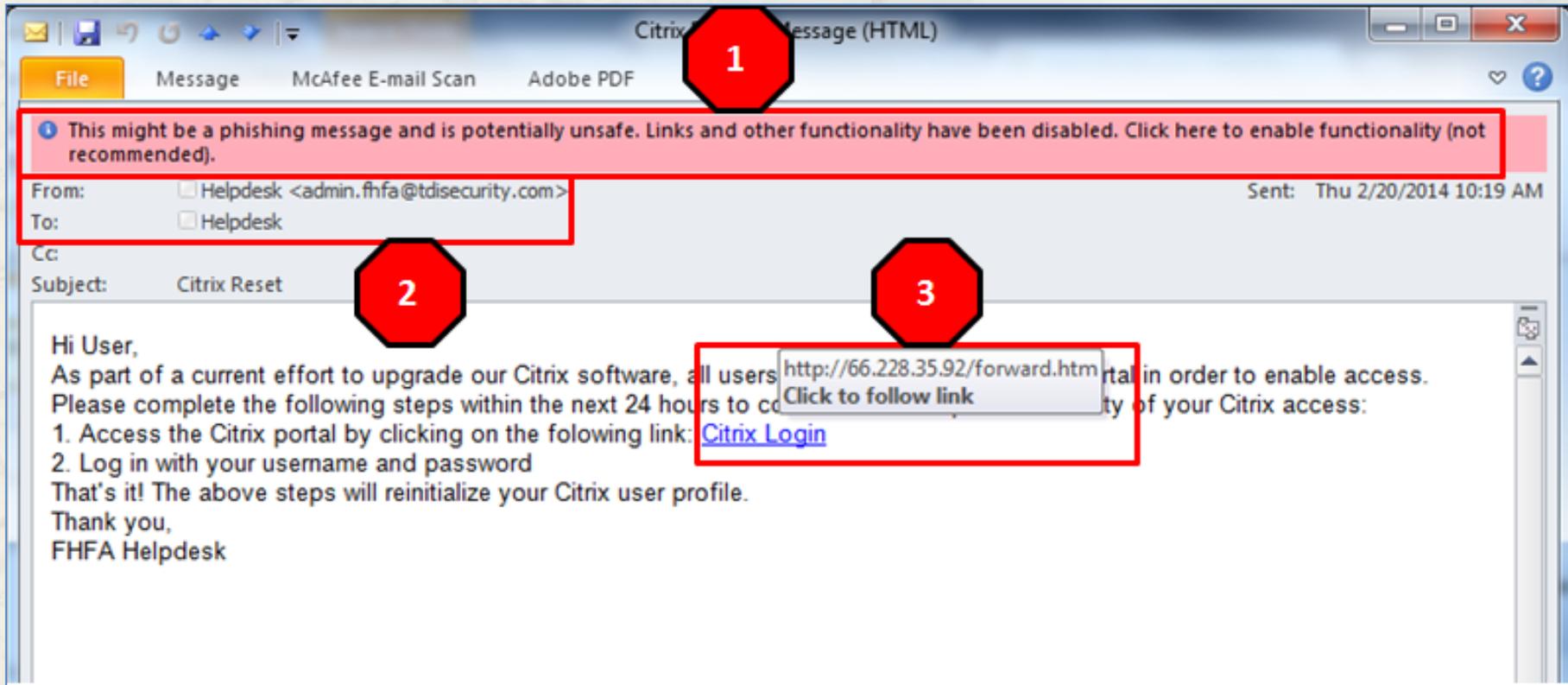
- Sony - Five unreleased movies, an estimated 38 million files of corporate information, and personal information of employees and stars.
- Anthem – 78.8 million records exposed containing customer and employee names, birth dates, Social Security numbers, addresses, email addresses and member IDs.
- Snapchat – Payroll department was targeted by someone impersonating their CEO who asked for employee payroll information.
- Spear phishing attacks continues to be the biggest threat to federal agencies.
  - 91% of cyberattacks begin with spear phishing email <sup>1</sup>

Note: <sup>1</sup> *Email: Most Favored APT Attach Bait*, Trend Micro Research Paper 2012.

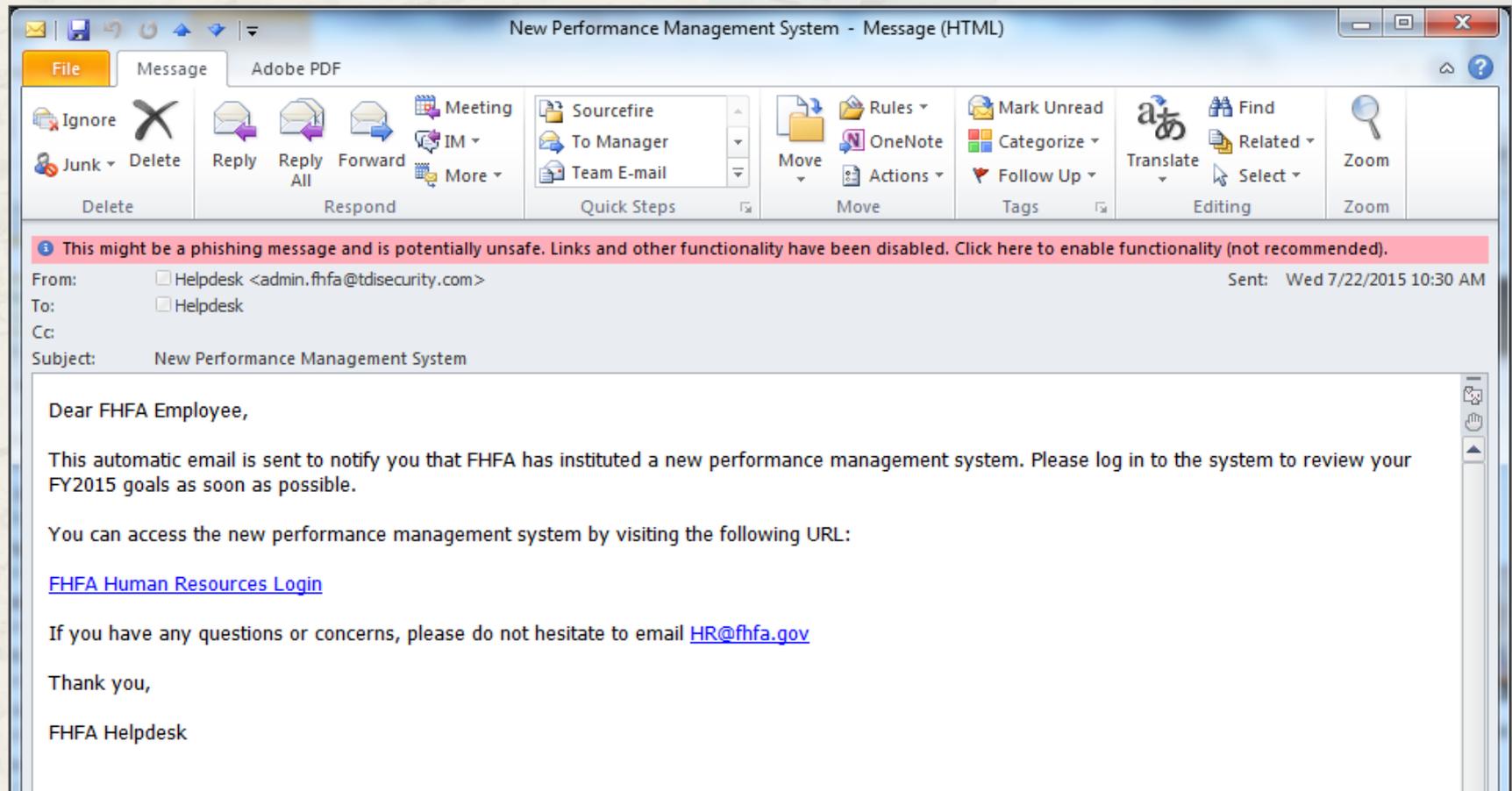
# THE SOCIAL ENGINEERING EXPERIMENT

- Security conducted three social engineering tests in three years.
- Phishing emails were sent from outside the FHFA network notifying users to change their passwords and announcing a new Performance Management System.
- USB devices were left on different floors with sample salary data.
- A fake Website was set up to track results.

# THE EMAIL - 2014!!!!

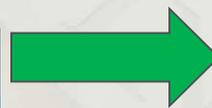
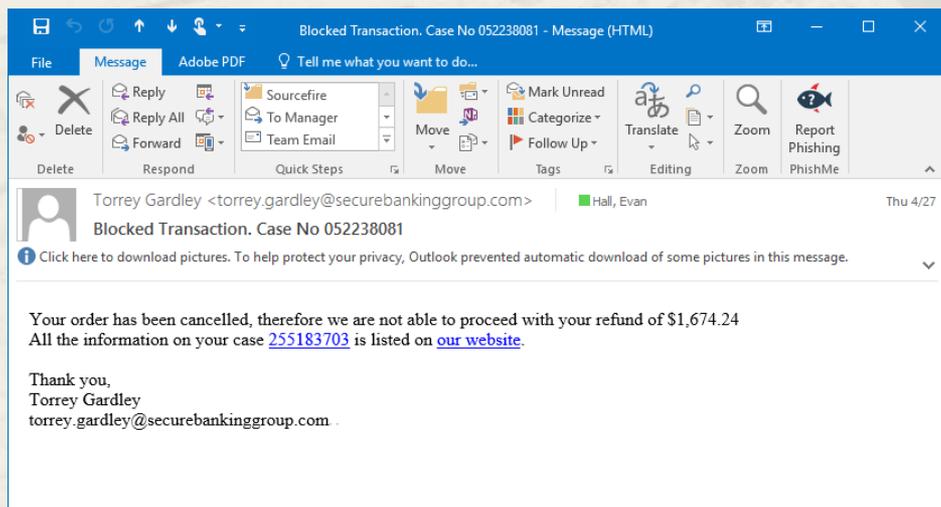


# THE EMAIL - 2015!!!!



# Phishing Awareness Campaign

- FHFA recently purchased an anti-phishing tool called “PhishMe” which allows phishing simulation attacks using real-world examples as a way to educate users and assess FHFA’s susceptibility to common phishing attacks.
- FHFA’s first exercise using PhishMe was based on a real phishing email that was used to distribute “Sage” ransomware.
- All FHFA users received an email alerting them of a cancelled refund, with two hyperlinks that, if clicked, alerted the user that this was an FHFA exercise, and presented them with awareness information on common phishing techniques.



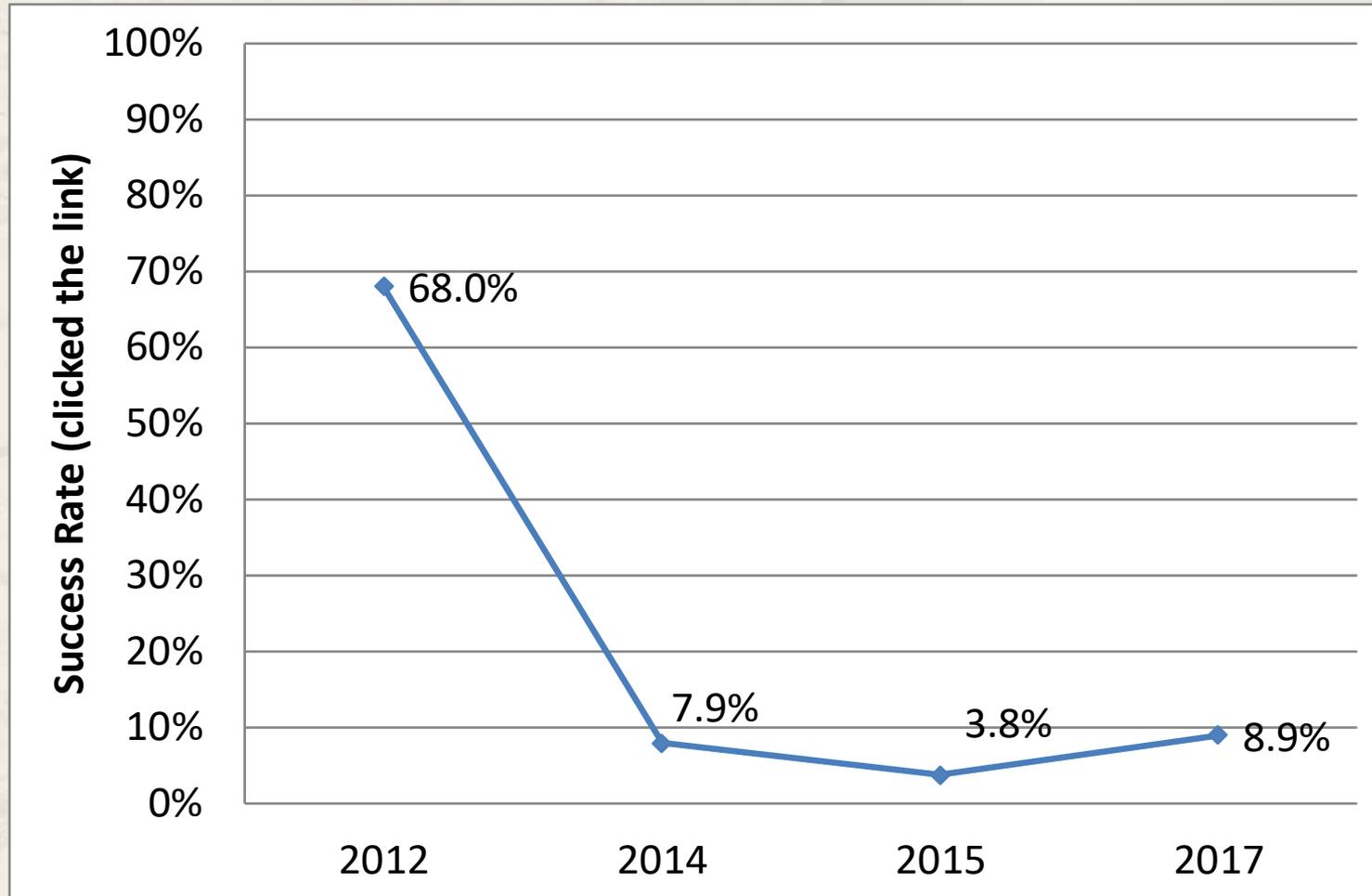
This has been an FHFA authorized simulation designed to teach you about spear phishing threats. Please take the time to learn how you can help prevent this type of attack.



# Phishing Exercise Results by Year

- April 2012
  - ❑ 23 out of 34 users clicked on the embedded link (68%)
  - ❑ 32% of the users who received this e-mail either deleted it, ignored it, reported it to the Help Desk, or sent e-mails to OTIM Security.
- February 2014
  - ❑ 53 out of 668 users clicked the embedded link (7.9%)
  - ❑ 92.1% of the users who received this e-mail either deleted it, ignored it, reported it to the Help Desk, or sent e-mails to OTIM Security.
- July 2015
  - ❑ 26 out of 679 users clicked the embedded link (3.8%)
  - ❑ 96.2% of the users who received this e-mail either deleted it, ignored it, reported it to the Help Desk, or sent e-mails to OTIM Security.
- April 2017
  - ❑ 64 out of 718 users clicked the embedded link (8.9%)
  - ❑ 91.1% of the users who received this e-mail either deleted it, ignored it, reported it to the Help Desk, or sent e-mails to OTIM Security.

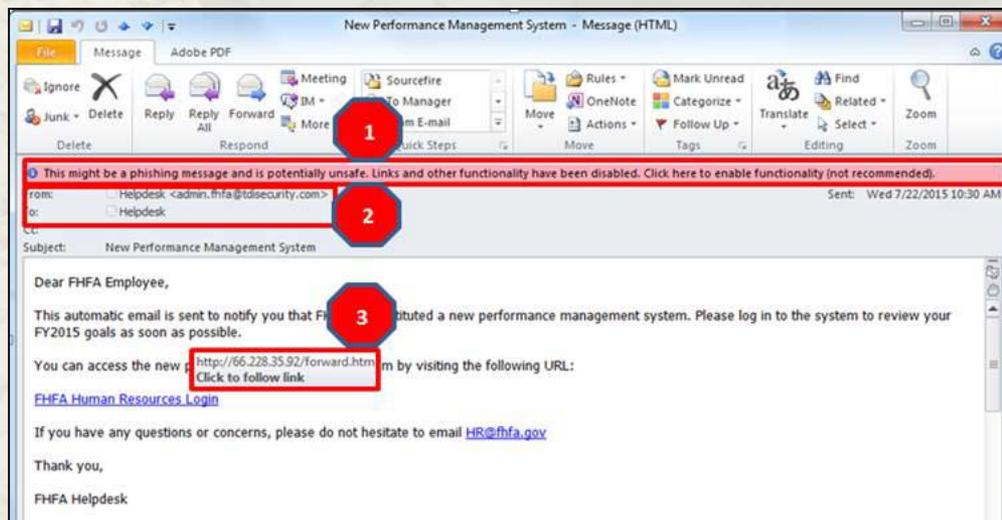
# FHFA Phishing Susceptibility Over Time



# HOW CAN YOU BE VIGILANT

## *How to identify potential email phishing attempts:*

- Outlook Warning Messages: Outlook will flag suspicious messages. This warning message is a strong indicator of a suspicious message, but is not guaranteed to catch every malicious email.
- Examine the “From” and “To” Address
- Examine Hyperlinks



# FINAL THOUGHTS ...

- End users are your first line of defense so leverage them.
  - Have them report suspicious activity to the appropriate office.
- Your training approach may require a cultural change.
- Know your audience and tailor your program for your end users.
  - Baby Boomers (1946-1964) vs. Gen X (1965-1979) vs. Millennials (Gen Y; 1980 – 2000) vs. Gen Z (post 2000)
- Raise awareness by using different training techniques.

# FINAL THOUGHTS (CONT)...

- Take small steps when necessary.
- Measure your training effectiveness.
- Be proactive and look for different training techniques and mechanisms.
- *Invest in your cybersecurity training program, it's a cost-effective way to protect your network.*

QUESTIONS?????

**Ralph Mosios**  
**e-mail: [ralph.mosios@fhfa.gov](mailto:ralph.mosios@fhfa.gov)**  
**(202) 649-3680**





# Upcoming Events





## ISC2 Richmond Metro Chapter Meeting

- Meetings for the ISC2 Richmond Metro chapter are typically held on the last Thursday of the month.
- This month's meeting is June 29<sup>th</sup> at the ECPI location, 800 Moorefield Park Drive, Richmond, VA 23236 from 6 pm to 8 pm
- Please sign up for the newsletter here:  
<http://isc2chapter-richmondmetro.com/>



## IS Orientations

### Current Schedule:

- June 22 1 pm to 3 pm
- Sept 21 9 am to 11 am
- Dec 14 1 pm to 3 pm

### Link for registration:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



## OSIG Audit

- Objectives:
  1. Executive branch agencies have identified all sensitive systems and whether they have accurately reported that information to the Virginia Information Technologies Agency (VITA).
  2. Non-sensitive systems exclude sensitive data as defined by the Commonwealth of Virginia Information Security Standard (ITRM Standard SEC501-09.1, December 8, 2016).
  3. The reporting structure of the Information Security Officers in the executive-branch agencies provides for independence and adequate separation of duties.
  4. Executive-branch agency budgets include a separate line item for Sensitive System Security Audits to prevent competition with other operational requirements.
  5. Executive-branch agencies are in compliance with Commonwealth of Virginia Information Technology Security Audit Standard (ITRM Standard SEC 502-02.3, December 8, 2016).
  6. Goals set by VITA to measure audit plan completion rates are reasonable.



## OSIG Audit

Your agency may be contacted by OSIG or Cotton & Company CPAs during the course of this audit.

Please give them your full cooperation.



## Future ISOAG

**July 5 ,2017 1:00 - 4:00 pm @ CESC**

**Speakers: Gene Fishel, OAG**

**&**

***Doug Mungle, Control Coach Consulting***

***ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2017***

# ADJOURN

## THANK YOU FOR ATTENDING

