



ISOAG Meeting June 1 , 2016

Welcome to CESC!





ISOAG June 1, 2016 Agenda

I. Welcome & Opening Remarks

Mike Watson, VITA

II. HIPAA- Understanding the Basics of Compliance

Jay Hodes, President of Colington Consulting

III. VITA IT Sourcing Project

Perry Pascual, VITA

IV. Phishing Exercise Update

Andy Burge, VITA

V. Shared ISO/Auditing Service Update

Ed Miller, VITA

VI. Upcoming Events

Mike Watson, VITA

VII. Partnership Update

Northrop Grumman



Welcome and Opening Remarks

Michael Watson

June 1, 2016

HIPAA



Understanding the Basics of Compliance



This presentation is educational and not a solicitation for services

My Background



- 27 years in Federal Law Enforcement
- 18 years at HHS, former Assistant Inspector General for Investigations.
- 35 years of combined experience in risk assessments, site security evaluation, regulatory compliance, policy and procedures assessments, and management.
- President & Founder, Colington Consulting
- Philosophy: **Apply a reasonable, scalable, and common sense approach to HIPAA compliance.**



LINCARE INC TO PAY \$239,800 CMP FOR HIPAA VIOLATION



MAN INDICTED FOR 5 YEAR IDENTITY THEFT SPREE USED MEMPHIS NEUROLOGY DATA



CYBERATTACKERS DEMAND \$3.6M RANSOM FROM HOLLYWOOD HOSPITAL



LOUISIANA HEALTHCARE CONNECTIONS BREACH AFFECTS 13K MEDICAID RECIPIENTS



ROGUE EMPLOYEE STEALS 24000 JACKSON HEALTH SYSTEM PATIENT RECORDS

Health Information Security Workshop



Instructor: “No, it is not a female hippopotamus, does any one else know?”

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- HIPAA is the federal statutory basis for the establishment of national standards for the privacy and security of protected health information (PHI)
- Why it was created



What is HITECH?

- **Health Information Technology for Economic and Clinical Health Act**
- Created in 2009 to stimulate the adoption of electronic health records (EHR) and supporting technology
- President Obama signed HITECH into law on Feb. 17, 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA) economic stimulus bill.



What is HITECH?

- Promotes the adoption and meaningful use of health information technology.
- Addresses the privacy and security concerns associated with the electronic transmission of health information.
- As it was originally enacted, HITECH stipulated that, beginning in 2011, healthcare providers would be offered financial incentives for demonstrating "meaningful use" of EHRs until 2015, after which time penalties may be levied for failing to demonstrate such use.



HIPAA & HITECH

- Are separate and unrelated laws
- They do reinforce each other in certain ways
- HITECH stipulates that technologies and technology standards created under HITECH do not compromise HIPAA privacy and security laws.



HIPAA Omnibus Rule

- **Expands patient rights by allowing them to ask for a copy of their electronic medical record in electronic form.**
- **When patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan.**
- **Prohibits the sale of an individuals' health information without their permission.**

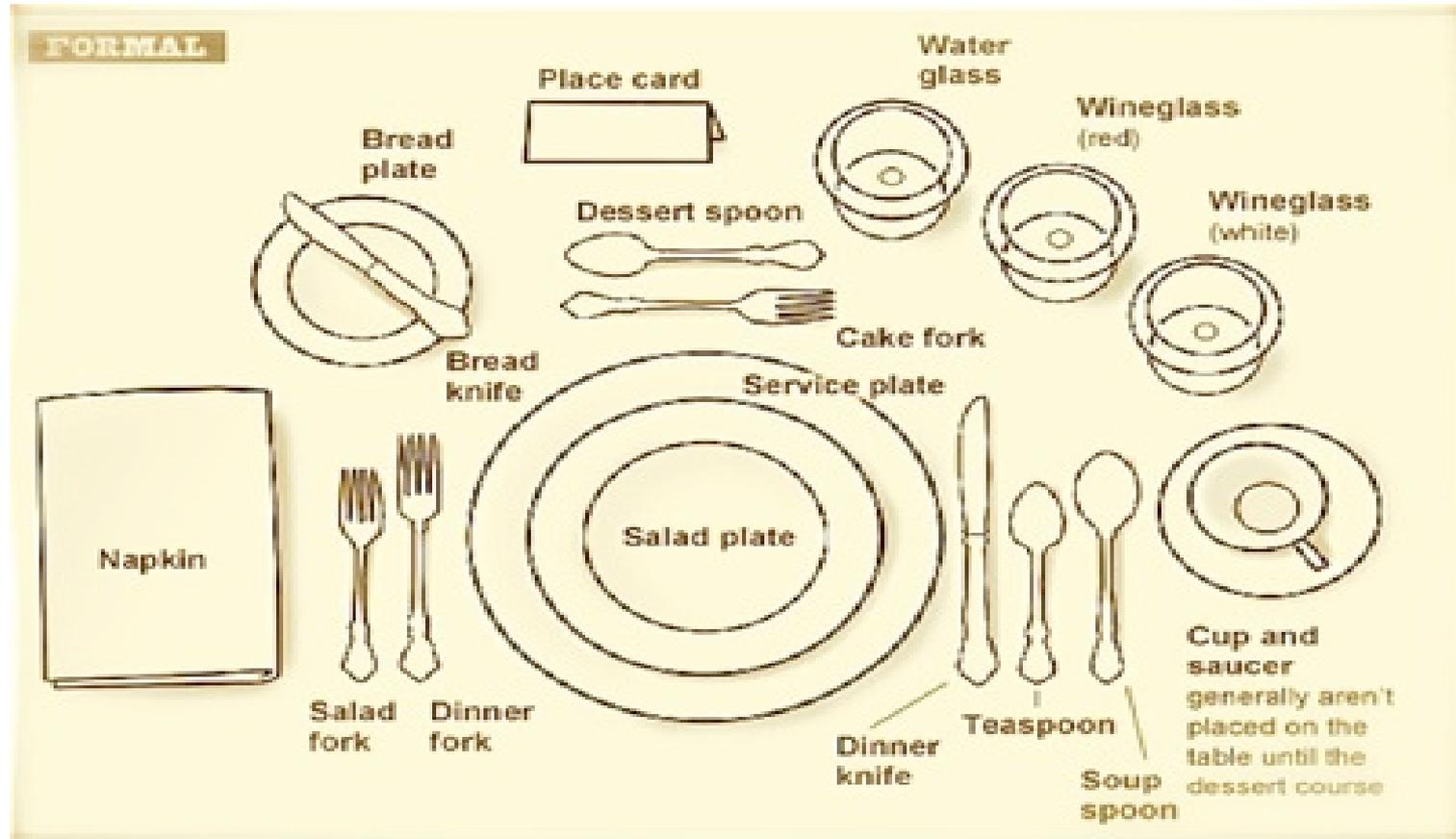


RISK MITIGATION

- It is steps taken to control or prevent a hazard from causing harm and to reduce risk to a tolerable or acceptable level.
- **HIPAA is about mitigating the risk of a potential breach of protected health information.**



Setting the HIPAA Table



What is Protected Health Information (PHI)?

- Individually identifiable health information that is:
 - transmitted by electronic media;
 - maintained in any electronic medium;
 - or transmitted or maintained in any other form or medium.
 - sent or stored in any form (written, verbal or electronic)
- There are 18 specific identifiers of PHI information that include: patient names, addresses; medical record numbers; Social Security numbers; account numbers; email addresses; beneficiary numbers; fingerprints or photographic images.



What is Electronic Protected Health Information (ePHI)?

Refers to any protected health information (PHI) that is covered under HIPAA regulations and is produced, saved, transferred or received in an electronic form.

What is the HIPAA Privacy Rule?

- The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other protected health information (PHI), especially in light of electronic healthcare transactions.
- **Creates safeguards that must be used to protect PHI.**
- Sets limits on the use and release of health records.



What is the HIPAA Security Rule?

- Sets the security standards for the protection of electronic protected health information.
- Requires the implementation of administrative, **technical** and physical safeguards to ensure the secure passage, maintenance and reception of PHI.



Who Must Follow the Security Rule?

Federal regulations identify two categories of individuals, organizations, agencies, and businesses that must comply with HIPAA requirements. Those are:

➤ **Covered Entities**

➤ **Business Associates**

Covered Entity

- Any provider of medical or other healthcare services or supplies that transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- This includes Health Plans and Healthcare Clearinghouses that perform electronic health care billing functions.
- Accept Medicare/Medicaid patients.

Examples of Covered Entities

- Hospitals
- Health Care Providers
- Dentists
- Health Plans / HMOs
- Outpatient Facilities
- Pharmacies
- Private Practices
- Mental Health Centers
- Skilled Care Facilities



Business Associate

With certain exceptions, a person or entity that:

- Creates, receives, maintains, or transmits PHI for a function or activity regulated by the Privacy Rule for a Covered Entity;
- Provides **IT services, cloud storage**, legal, actuarial, accounting, consulting, **data collection and analysis**, management, administrative, **accreditation**, or financial services to or for a Covered Entity and **will have access to PHI**.



Examples of Business Associates

- **Medical transcription companies**
- Answering services
- **Document storage or disposal (shredding) companies**
- Patient safety or accreditation organizations
- Companies involved in claims processing, repricing or collections (e.g., medical billing companies)
- Health information exchanges (HIEs), e-prescribing gateways and other HIOs
- Third party administrators and pharmacy benefit managers
- Data conversion, de-identification and data analysis service providers
- Utilization review and management companies
- **Web site hosting companies IF maintaining patient forms with PHI**



Concerns for Business Associates

- Must comply with a wide-range of regulatory obligations, including certain privacy obligations, security standards, and breach notification requirements.
- **Must enter into a Business Associate Agreement (BAA) with a Covered Entity.**
- Must enter into a BAA with subcontractors that access PHI.
- **Subject to audits, investigations, and civil monetary penalties for violations by the U.S. Department of HHS (Omnibus Rule).**

Business Associate Agreements



Indemnification Clauses

Vendor/BA Security Questionnaires

- **Trending in the healthcare sector**
- **Covered Entities should use, BA should be prepared to answer these questionnaires**

Example of Questions:

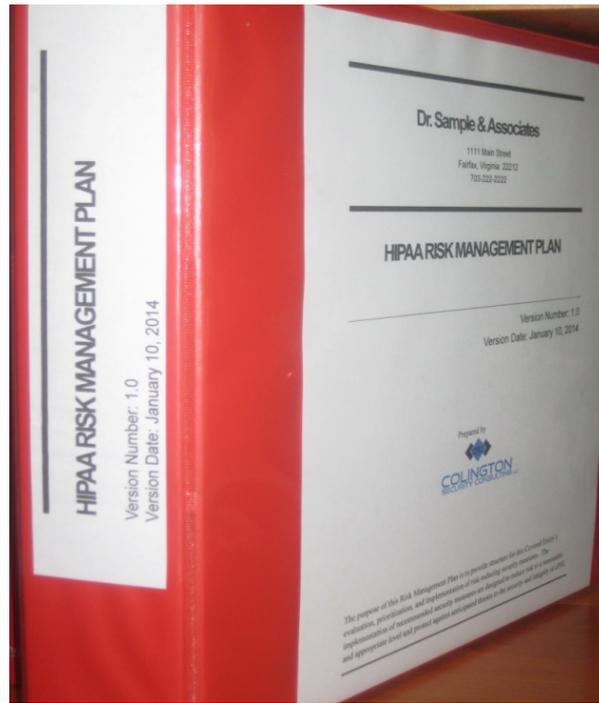
- Does your organization identify all information systems that create, receives, maintain, transmit and ePHI?
- Does your organization identify all hardware and software that maintains or transmits ePHI, including Excel spreadsheets, Word (or similar) documents, and other data storage and included it in your inventory?





Copyright ©2013 R.J. Romero.

"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."



Document, Document, Document

3 Major Components of a HIPAA Compliance Program

- **HIPAA Risk Management
Plan (Policies and Procedures)**
- **HIPAA Risk Assessment**
- **HIPAA Security Awareness
Training**

Risk Management Plan Must Cover:

Administrative Safeguards

Technical Safeguards

Physical Safeguards

General Policies And Procedures



What are Administrative Safeguards?

- Policies and procedures that direct the conduct of the workforce.
- Actions put in place to protect PHI.
- **ADMINISTRATIVE SAFEGUARDS** includes:
 - ❖ Contingency Plans
 - ❖ Use of Business Associate Agreements
 - ❖ Workforce Security Measures
 - ❖ Information Management Access

HIPAA Risk Assessment

- **Compliance Requirement**
- **Determines Vulnerabilities and Threats**
- **Gap Analysis**
- **Remediation – Actionable Items**



Remediation Follow Up

- Prioritize are all HIGH risks, followed by MEDIUM
- Systematic way to track remediation
- Follow up time frames (15, 30, 60, 90 days)
- Who is assigned remediation?
- Hold accountable!!
- **Is the risk mitigated?**

HIPAA Security Awareness Training

Must Cover: 4 Implementation Specifications:

- Security Reminders
- Protection for Malicious Software
- Log-In Monitoring
- Password Management

Should Cover: HIPAA Privacy & Security Rules

- Annual Requirement

What are Physical Safeguards?

- A set of rules and requirements that focus on physical access to PHI.
- Protection from unauthorized access to sensitive data and records.
- PHYSICAL SAFEGUARDS include:
 - ❖ Facility Access Controls
 - ❖ Workstation Use
 - ❖ Workstation Security
 - ❖ Device and Media Controls
 - ❖ Keeping file cabinets, doors, and desks locked in areas where PHI is maintained or is accessible.





- **Data at Rest**
- **Data in Use**
- **Data in Transmission**

What are Technical Safeguards?

- Focus on the technology that protects PHI.
- Procedures to control and audit access.
- TECHNICAL SAFEGUARDS includes:
 - ❖ Unique User Identification
 - ❖ Integrity of ePHI
 - ❖ Transmission Security
 - ❖ Encryption

Data Cybersecurity & HIPAA

- **To reduce risks to ePHI, Covered Entities and Business Associates must have the proper safeguards in place.**
- **Requirements for health information technology includes policy and procedure for:**
 - **Data Backup & Storage**
 - **Transferring & Downloading Data**
 - **Data/Media Disposal - Sanitation and Document Destruction Reports must be maintained**

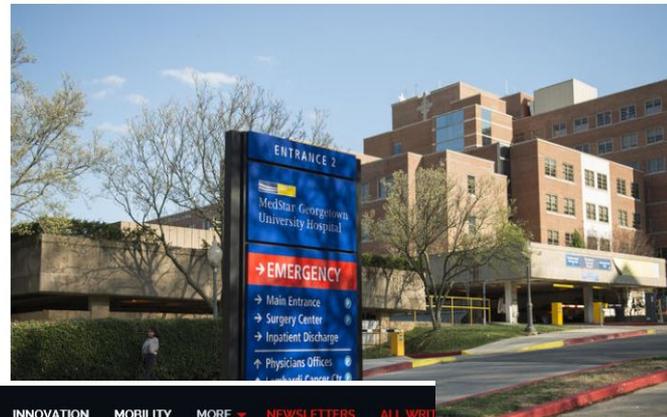


Hollywood hospital pays \$17,000 in bitcoin to hackers; FBI investigating



The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extorrior hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access. (Ric Los Angeles Times)

MedStar hack shows risks that come with electronic health records



forcing records systems offline for thousands of d the health care sector. (Molly Riley / AP)



SEARCH



CLOUD

CXO

HARDWARE

WINDOWS 10

IOT

INNOVATION

MOBILITY

MORE

NEWSLETTERS

ALL WRIT

MUST READ [HOW SMART STORAGE WILL RESCUE BIG DATA](#)

Ransomware is now the biggest cybersecurity threat

Simple attacks plus user willingness to pay ransoms to get their files back means ransomware is on the rise, warn Kaspersky researchers.





“Apparently you contracted a virus from your computer, so we had to erase your memory. I trust you have a backup copy?”

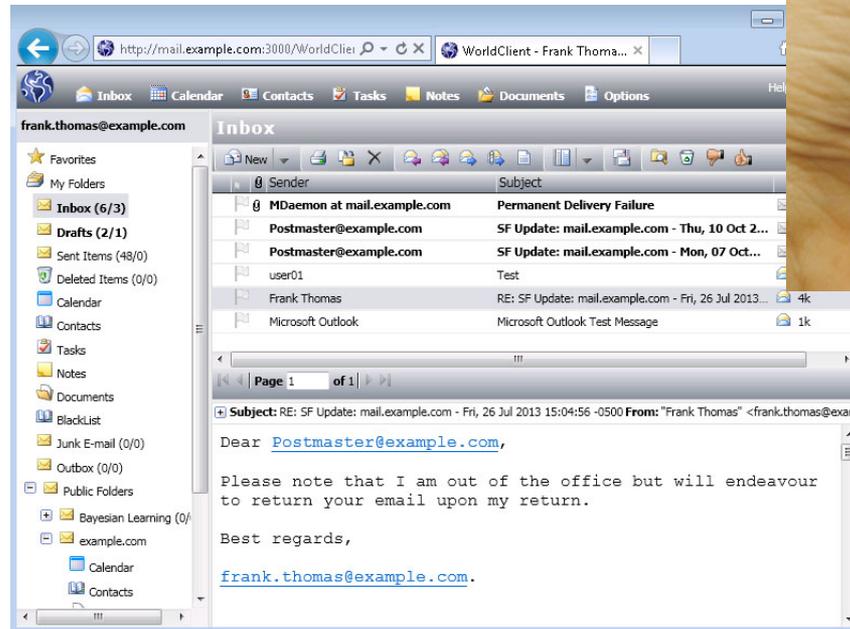
PHI & Can I?

- EMAIL

- TEXT

- FAX

- COPY



Does Your Agency have Comprehensive HIPAA Policies and Procedures for:

- Contingency Plans
- Disaster Recovery (IT and operational)
- Emergency Operations Mode

Good Business Practice

- Continuity of Business Operations



Who Enforces HIPAA Compliance?

- The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) enforces HIPAA compliance throughout the country.
- HIPAA can be enforced by the Attorney General of each state.





FTC's Health Breach Notification Rule

- Vendor of personal health records (PHRs);
- PHR-related entity; or
- Third-party service provider for a vendor of PHRs or a PHR-related entity
- **Starting investigation claims of “HIPAA Compliant”**

What are the Penalties for HIPAA Violations?

- Penalties for noncompliance are based on a level of negligence.
- Civil monetary penalties range from \$100 to \$50,000 per violation of each patient record.
- A maximum penalty of \$1.5 million per year for identical provisions.
- Criminal penalties can range up to 10 years in jail.



HIPAA Data Breach

A HIPAA data breach is a release of unsecured PHI to an unauthorized entity or in an insecure environment, whether intentional or unintentional.

This includes attempted or unauthorized access to use of information, or misuse of information, disclosure, modification, destruction of information, and interference with operations in an information technology system.





**Breaches affecting 500
or more individuals**

**Breaches affecting fewer
than 500 individuals**



Breach Notification Requirements for Business Associates

- Check BAA section for notification requirements
- Timeline to report to Covered Entity may be shorter



What has Caused HIPAA Breaches to Occur?

- **Data is not encrypted**
- **Computer or other mobile devices are lost or stolen**
- **PHI left in a public area, or accessible on a public computer or website**
- **Compromised Credentials**
- **Correspondence containing PHI transmitted to the wrong address (email – fax)**
- **Documents and hard drives containing PHI are not properly destroyed**



Medical identity thefts account for **43%** of all reported identity theft cases in the U.S.*



* Source: [FBI](#)

57% of reported health care breaches involve a lost or stolen laptop or mobile device*



* Source: [U.S. Department of Health and Human Services](#)

91,771,820*

Individuals Affected by Reported HIPAA Breaches March 2015

* Source: [U.S. Department of Health and Human Services
Breach Notification Portal](#)

Breach Highlights*

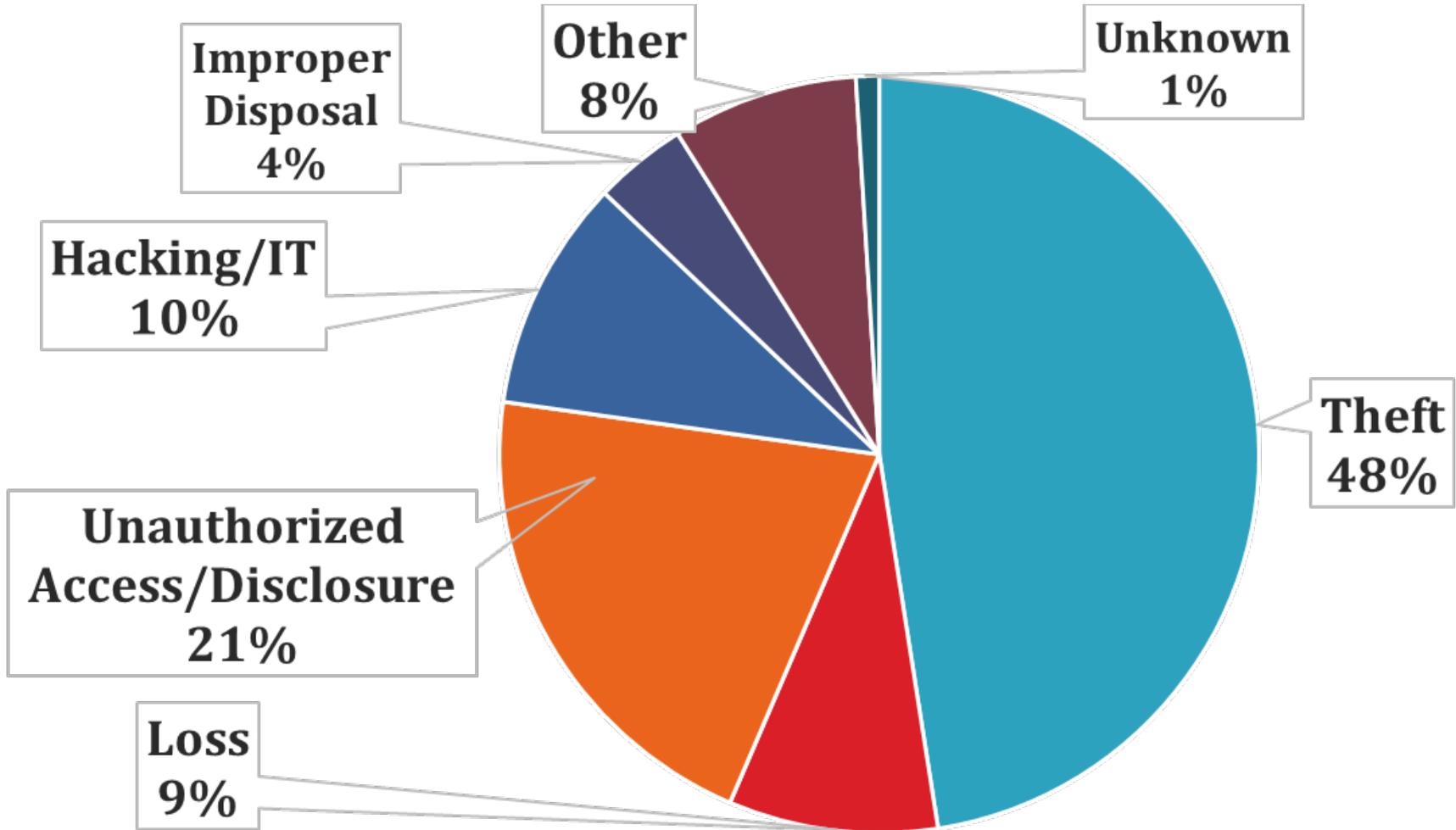
September 2009 through August 28, 2015

- Approximately 1,310 reports involving a breach of PHI affecting 500 or more individuals
- Approximately 179,000+ reports of breaches of PHI affecting fewer than 500 individuals

* Source: [U.S. Department of Health and Human Services](#)

How Did the Breach Occur?

As of 8/31/15



HIPAA Violations Case Examples





- **\$90,000 Fine imposed by the Connecticut Attorney General**
- **Theft of unencrypted laptop from employee of a company EMC acquired**
- **Company performing data analysis for Hartford Hospital**
- **Laptop had patient information**
- **No Business Associate Agreement in place**

Skagit County (WA) agreed to a \$215,000 monetary settlement.



Investigation opened after receiving a breach report that money receipts with electronic protected health information (ePHI) were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County.

Investigation revealed a broader exposure of protected health information involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases.

Investigation uncovered general and widespread non-compliance with the HIPAA Privacy, Security, and Breach Notification Rules.





Alaska Department of Health and Social Services

- **USB containing ePHI was stolen out of a vehicle belonging to an employee of the Alaska DHSS**
- **Investigation revealed the agency:**
 - **Did not have the proper policies and procedures in place to protect and safeguard ePHI**
 - **Did not complete a risk assessment**
 - **Did not provide the workforce HIPAA Security Awareness Training**
 - **Did not have the proper device and media controls**
- **\$1,700,000 Settlement**



Concentra



- **Among their services; occupational health, urgent care**
- **Multiple reported breaches**
- **Paid more than \$1.7 million to settle potential security violations**
- **Thefts of laptop computer that lacked data-protecting encryption**



- **Offices in MA & NH**
- **\$150,000 Fine**
- **Loss of an unencrypted thumb drive containing ePHI of 2,200 patients.**
- **Investigation revealed an accurate and thorough risk assessment not conducted.**



- **Offices located in Indiana**
- **Radiation oncology private physician practice**
- **\$750,000 Settlement**
- **Stolen laptop containing unencrypted ePHI of 55,000 patients.**
- **Investigation revealed wide spread non-compliance with the HIPAA Security Rule.**

Iliana Peters - OCR Senior Advisor for Compliance and Enforcement



Areas where some providers are struggling:

- The ability to monitor traffic on the firewall
- The need to continuously patch software
- The improper disposal of IT equipment (not sufficiently wiping or destroying)
- Insufficient data backup and contingency planning
- The ability to remote wipe devices if lost or stolen
- Making sure ALL ePHI is backed up in case of ransomware attacks
- Making sure ALL ePHI is backed up in case of natural or man-made causes
- Making sure if possible ALL ePHI at rest is encrypted in all media platforms

Education, Awareness and Training

- ✓ **Policies and Procedures (HIPAA Risk Management Plan)**
- ✓ **Compliance Program Management**
- ✓ **Risk Assessments**
- ✓ **Data and Network Protection**
- ✓ **Data Retention and Disposal**
- ✓ **Facility Security Plan**
- ✓ **Patient Privacy Protection**
- ✓ **Business Associate Agreements**
- ✓ **Access Authorization Procedures**
- ✓ **Information Sharing and Transmission**



Summary

- **A great HIPAA compliance program starts with you and your commitment to protect confidential and protected health information.**
- **Everyone has a role in making this happen.**
- **FAILURE TO COMPLY WITH HIPAA REGULATIONS CAN CAUSE:**
 - **Loss of overall trust, workforce trust and public trust.**
 - **Embarrassment and poor publicity for organization.**
 - **Potential for fines and criminal prosecution by State and Federal government.**



Create a Culture of Compliance



**I DON'T ALWAYS FOLLOW
HIPAA STANDARDS...**





Jay Hodes

202-669-1140

jhodes@colingtonsecurity.com

<http://colingtonsecurity.com>



Virginia Information Technologies Agency

Perry Pascual, VITA

VITA IT Sourcing Project



Virginia Information Technologies Agency

Infrastructure Services Sourcing

Perry Pascual

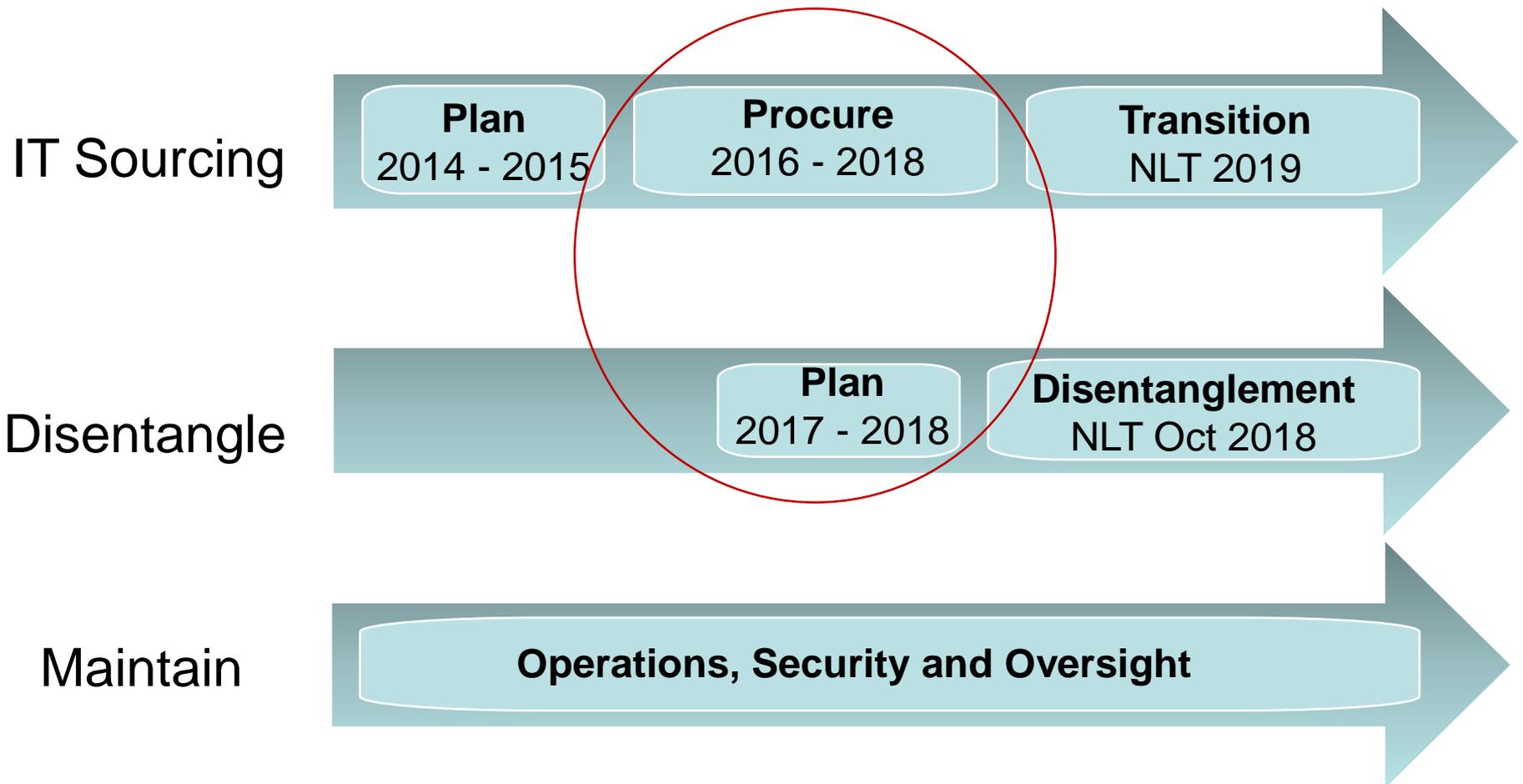
Director, IT Sourcing Strategy

June 1, 2016

ISOAG



Current Timelines





Goals for Future Services Delivery Platform

Agencies

- Service delivery quality
- Ease of doing business
- Service flexibility
- Innovation and evolution
- Agency choice
- Service transparency
- Spend transparency

Enterprise

- Maintain cost competitiveness
- Management control
- Flexibility to evolve
- Supports VITA oversight functions
- Standardization
- Security
- Procurement and Transition



Current Activities

- Preparing for transition and disentanglement
- Starting to build multi-supplier model, including a services integrator
- Contemplating organizational adjustments to support these changes
- Working with Customer Advisory Council (CAC) to enhance agency involvement in future services delivery platform



Summary Timeline

Define high-level scope, initiate MSI and selected tactical procurements, begin NG negotiations, sign contracts first wave of contracts.

Transition to new service providers, implement new service levels and reporting, establish updated service catalog, interim governance model.

Refine and evolve the platform – identify new services, re-procure remaining infrastructure towers, finalize governance model.

Build

Stabilize

Platform Extension

2016

2017

2018

2019

Calendar Years

MSI Procurement

Remaining Tower Procurements

Tactical procurements

Contract Transitions

Tower Transitions

NG Negotiation

Process Improvement

Note: Contract disentanglement phase starts in October 2018 and runs through June 2021

Contract Disentanglement (through Jun 2021)

Recommended plan is to begin disentanglement early and have new operating model established in July 2019

Recommended Disentanglement (start early and end by Jun 2019)

First Wave

Second Wave

Third Wave



Status and Progress

- Messaging services competitive procurement in process
 - Planned award date June 30
- IBM mainframe services competitive procurement in process
 - Proposals received May 5
 - Planned award date July 29
- Chargeback applications in-source in process
 - Aligning to wave two
- Microsoft licensing in-source in process
 - VITA preparing for both future subject-matter expertise and program approach



Status and Progress continued

- Services delivery platform governance change in process
 - Platform relationship organization and related VITA changes
 - Agency interaction model (AIM) recommendations and plan
- Wave two and three strategy sessions in process
 - Inputs to wave two and three competitive procurements
 - Wave two competitive procurements begin in FY17
- Comprehensive Infrastructure Agreement (CIA) disentanglement



Guiding Principles

- Transition all services from Northrop Grumman contract by June 2019 (term)
- Manage implementation, operational and transitional risk
- Conduct multiple waves of procurements to mitigate operational and implementation risk
- Include agencies in request for proposal (RFP) development and evaluation



Guiding Principles continued

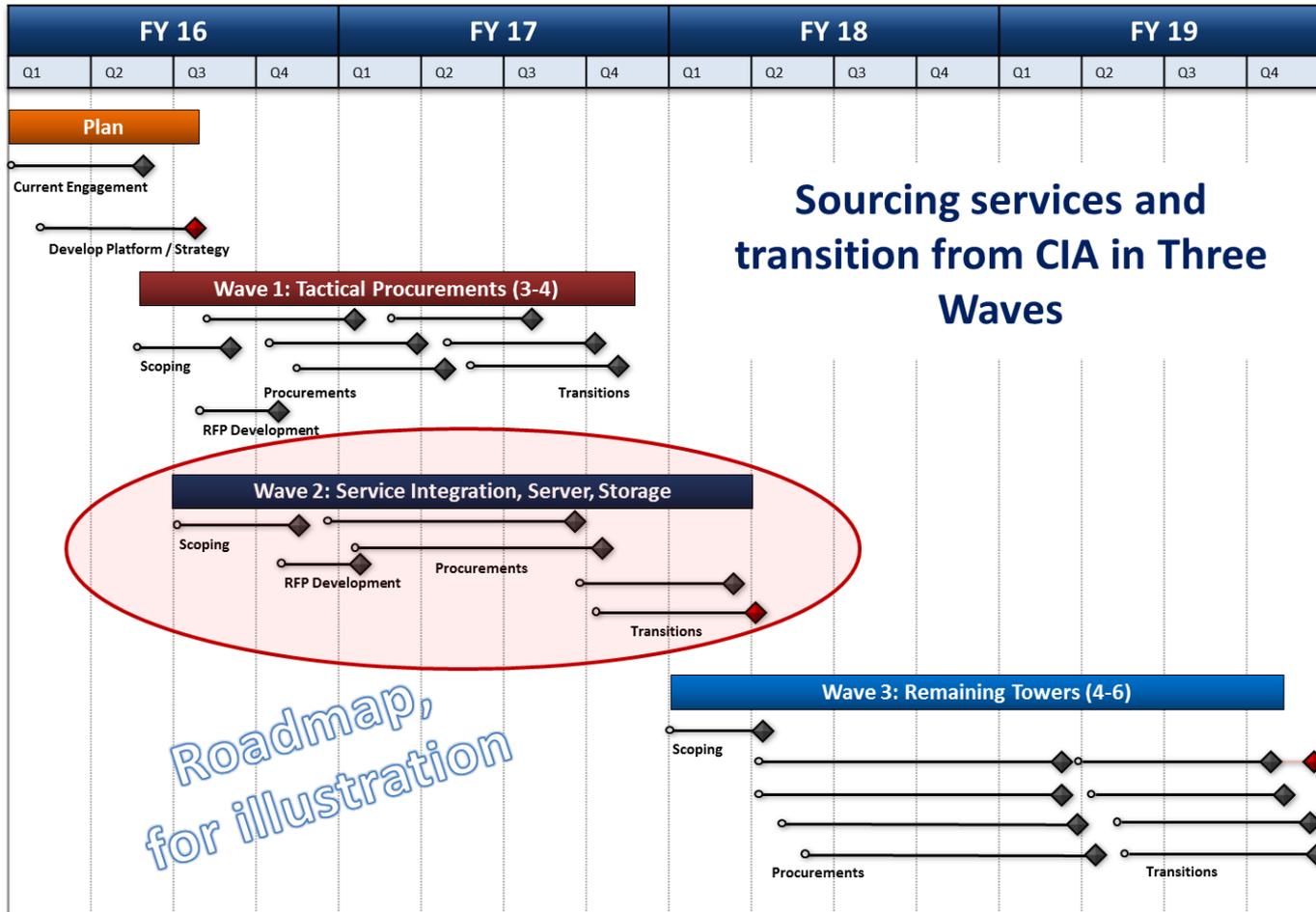
- Determine final solutions and integration points via RFP processes – not all decisions must be made now
- Maintain financial balance of service towers to create flexibility for the commonwealth
- Create competition within service towers whenever possible
- Create buying ability for at-will customers whenever possible



Program Competitive Procurements

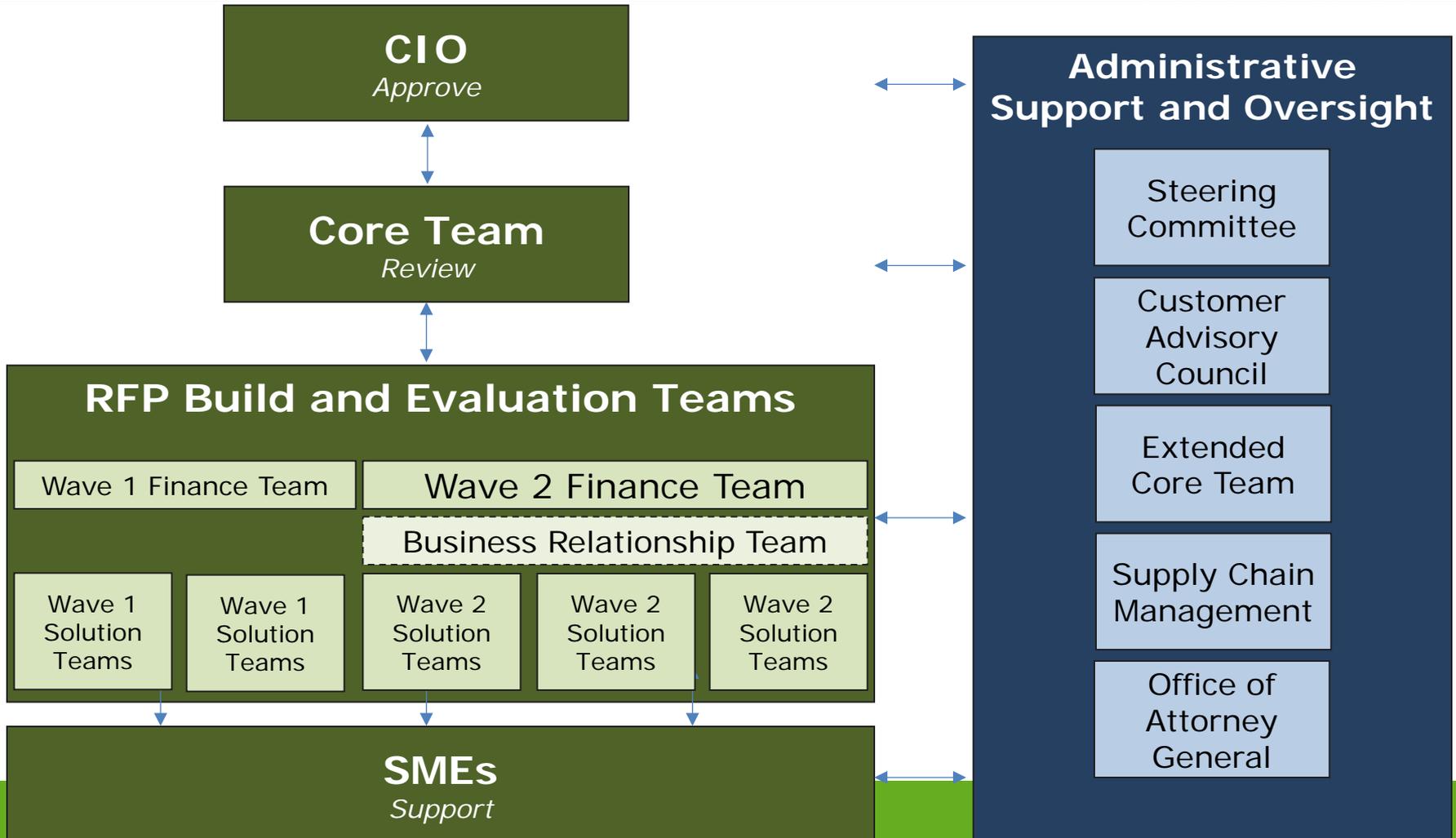
Wave	Service	RFP Issue Date (Notional)	Responses Due (Notional)	Service Commence (Notional)
1	Messaging	Feb 2016	April 2016	Nov 2016
	IBM Mainframe	March 2016	May 2016	Dec 2016
2	Service Integration / Service Desk	Aug 2016	Oct 2016	Nov 2017
	Server / Storage	Aug 2016	Oct 2016	Nov 2017
	Security	Sep 2016	Nov 2016	Nov 2017
3	Desktop	Aug 2017	Oct 2017	July 2019
	Data / Voice Networks	Feb 2018	April 2018	July 2019

Services Sourcing and Transition





RFP Teams





Broad Agency Participation

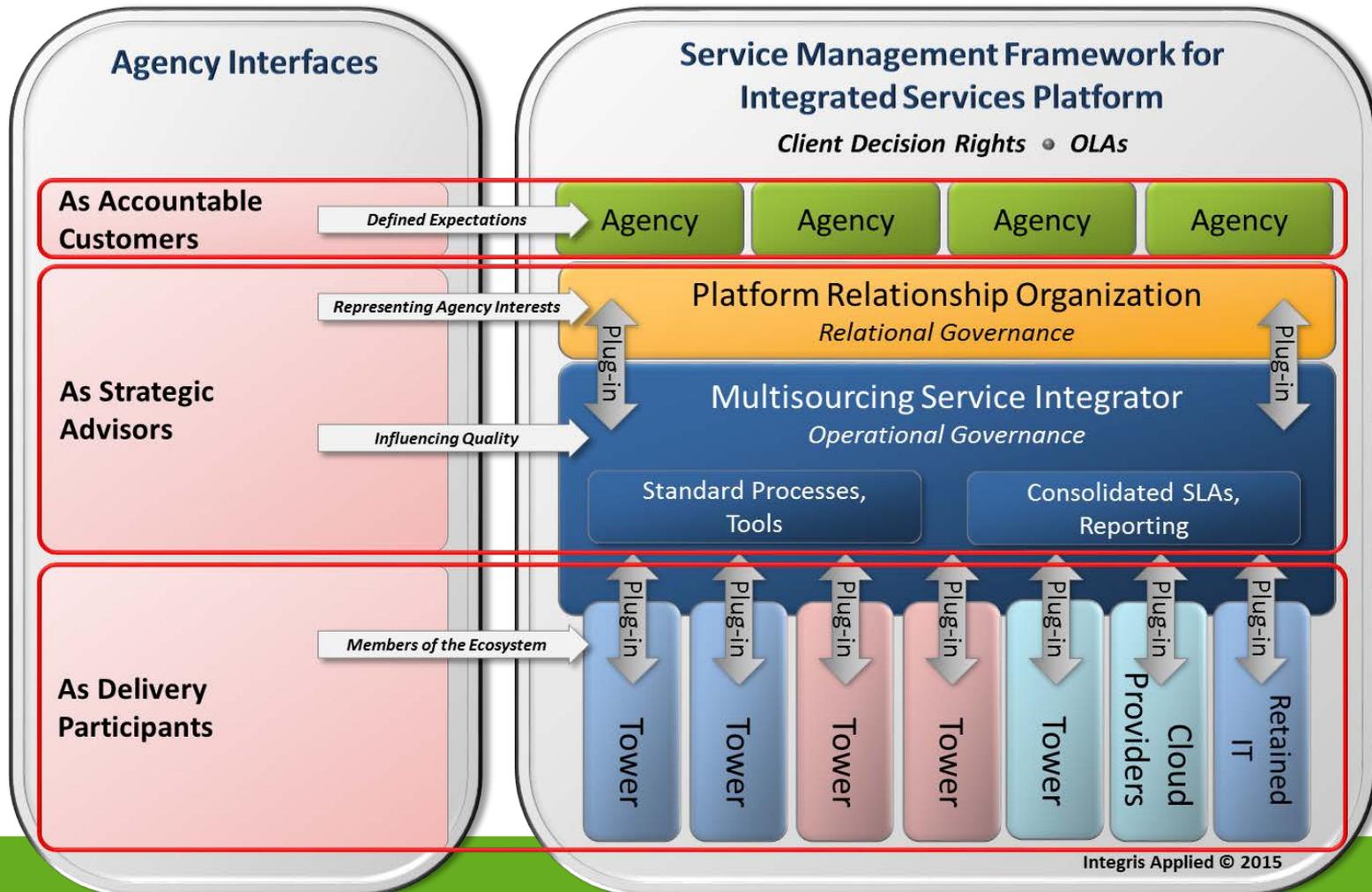
- Steering committee (four)
- Extended core/program management (three)
- Wave one RFP teams
 - Messaging (eight)
 - IBM mainframe (eight)
 - Finance (three)



Broad Agency Participation

- Wave two RFP teams
 - Business team/strategy sessions (eight)
 - Multi-source integration (six)
 - Server/storage (six)
 - Security (TBD)
 - Finance (four)
- Platform oversight/governance – CAC (15)
 - Ongoing agency representation for relational and operational governance
 - Contacting peer states

Agency Interaction Model (AIM)



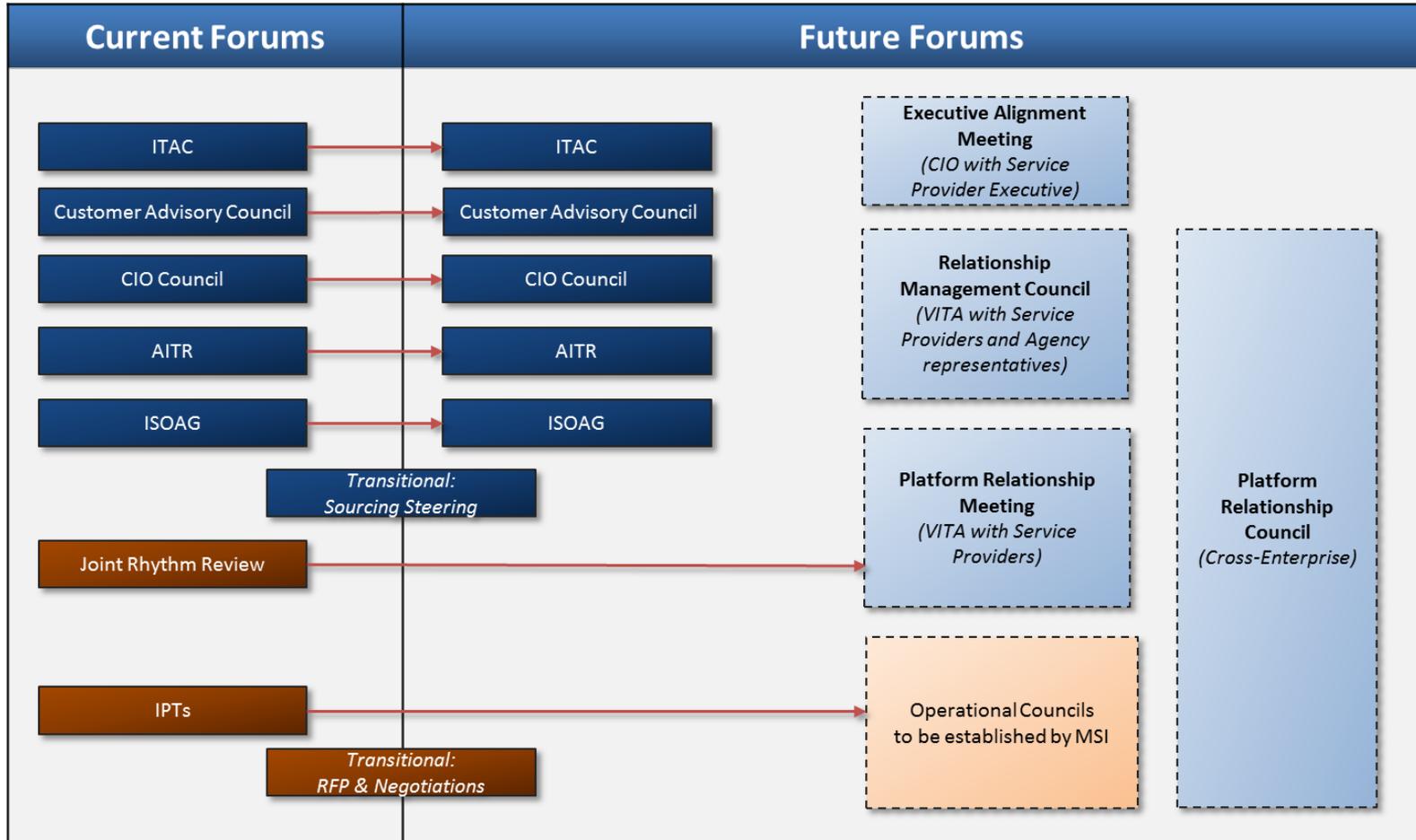


AIM Work Group

- CAC recommended a work group
 - Established and met April 29
 - New participants – Level setting including value of improved governance
 - Call with Georgia May 11
 - Working toward generating inputs for MSI and remaining wave two and three procurements
- Future agenda
 - Review enterprise and agency goals
 - Review AIM as proposed by Integris (four forums)
 - Review takeaways from Georgia call



Governance Forum Recommendations





Resources

- Information
[vita.virginia.gov](http://www.vita.virginia.gov) at this icon

IT Infrastructure Sourcing



<http://www.vita.virginia.gov/default.aspx?id=6442473400>

- Feedback and questions
infrastructuresourcing@vita.virginia.gov



Virginia Information Technologies Agency

Andy Burge, VITA Phishing Exercise Update



Phishing Attacks – May 2016

COV was hit with excessive amount of Phishing attacks..

From: Internal User (COV)
Sent: Wednesday, May 04, 2016 11:22 AM
Subject: IT Department

<http://site9265020.92.webydo.com>
Ctrl+Click to follow link

Please this message is important, we are expanding and upgrading all employee mailbox immediately. Please [CLICK HERE](#) and fill the form completely so we can upgrade and validate your mailbox. This message is from the helpdesk Department. If you cannot access the link, Please send your Email Address and Password to jeffreyanderson33@aol.com for immediate validation.

Helpdesk

Phishing Attacks – May 2016

- **64 COV users provided credentials**
- **41 compromised accounts contained before attacker access**
- **23 compromised accounts accessed by attacker and send thousands of internal Phishing emails**



Phishing Attacks – May 2016

Situation..

- **After the 'Click Here' link was blocked, users responded - sending credentials in email responses**
- **Attacker leveraged compromised accounts with mass mailing scripts**



Phishing Attacks – May 2016

Short-Term Remediation..

- Improved the detection and containment process to be more efficient
- So far the volume has significantly decreased



Phishing Attacks – May 2016

Long-Term Remediation..

- **Add context specific references to this attack in your security training**
- **Two-Factor authentication (Summer/Fall 2016)**
- **Extend Web-Proxy protection off network**



Phishing Attacks – May 2016

Questions?



Centralized ISO & Security Audit Services

Ed Miller
IT Security Governance





General Assembly Session 2016

- HB30 was introduced to support the Governor's budget related to state agency cyber security.
- The bill B.1: "(VITA) shall operate an **information technology security service center** to support the information technology security needs of agencies "
- "Support for participating agencies shall include, but not be limited to, **vulnerability scans**, information technology **security audits**, and **Information Security Officer services**."



General Assembly Session 2016

3. Agencies electing to participate **in the information technology security service center** shall enter into a **memorandum of understanding** with (VITA). Such memorandums shall outline the services to be provided by the Virginia Information Technologies Agency and the costs to provide those services.



General Assembly Session 2016

"4. **Non-participating agencies** *shall* be required by **July 1** each year to *notify* the Chief Information Officer of the Commonwealth *that the agency has met the requirements* of the Commonwealth's **information security standards**. If the *agency has not met the requirements* of the Commonwealth's information security standards, the agency *shall report* to the Chief Information Officer of the Commonwealth *the steps and procedures* the agency is implementing in order to satisfy the requirements."



Participation in Shared Audit/ISO Services

- In the next few weeks, we will be contacting all agencies that we have identified as candidates for this service.
- Some agencies will be targeted for shared Audit services, others for shared ISO services, some for both.
- You will need to either choose to use the shared service OR present CSRM with an acceptable plan of action to bring your agency into compliance.



So What Does This Mean?

Starting July 1 2016, VITA will be provided with funds and personnel to perform 3 critical IT security services:

- Vulnerability Scanning Services
- Centralized IT Security Auditing Services
- Centralized Information Security Services



So What Does This Mean?

Vulnerability Scanning Services

We are anticipating that we will hire 2 full-time personnel and purchase related software tools to conduct vulnerability scanning of ***all*** publicly facing websites and systems that are operated by state agencies.



So What Does This Mean?

Centralized IT Security Audit Services

We are anticipating that we will hire 6 to 8 FT employees to conduct IT security audits of sensitive IT systems.

We will also out-source some IT security audit work to auditing firms.

We will use a risk-based approach to prioritize and schedule these audits based on agency needs.



So What Does This Mean?

Centralized IT Security Services

We will also hire 5-6 FT employees to work directly with agencies to bring agency IT security programs into compliance with SEC501. The services provided will basically include:

- System Security Plans
- Risk Assessments (identifying threats, risks, vulnerabilities)
- Risk Treatment Plans
- Business Impact Analysis
- Compliance with VITA documentation and submission policies



What will it cost?

- We have developed a pricing model for these services. We are required by law to charge for these services.
- Agencies must either use the centralized services or adequately provide their own resources.
- These services are available to all Executive branch agencies.



What will an “audit” cost?

IT Security Audit:

In order to keep it simple, we’re going to structure audits as either:

Small

Medium

Large

A single audit will cost in the range of
\$18,000 to \$45,000



What will “ISO services” cost?

Business Impact Analysis:

Depending on the size/complexity of the agency and its mission functions, a BIA will cost in the range of \$10,000 to \$40,000



What will “ISO services” cost?

System Security Plan (Risk Assessments/Risk Treatment Plans)

Depending on the size/complexity of a particular system, a System Security Plan for a single system will be in the range of \$6,500 to \$10,000.



What will “ISO services” cost?

On-going ISO Services and Support

We will also offer on-going support for your ISO function. This will take care of all annual maintenance to update BIAs, RAs, Risk Treatment Plans, and also the compilation and submission of certain required VITA compliance reports.

Pricing will vary according to the size/complexity of the project and should be in the range of \$4,700 to \$17,000 per year.



Department of Planning & Budget

- DPB has developed a funding program to reimburse agencies for some of the costs associated with using the centralized IT security services.
- DPB funding will vary according to each agency. Some will be covered more, some less.
- Contact the DPB analyst for your agency for more information.

Any Questions?





Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Wednesday, June 29, 2016

Time: 10:00 am to 12:00 pm

Where: CESC , Room 1221

Register here:

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



Future ISOAG

July 6, 2016 1:00 - 4:00 pm @ CESC

Speakers: Ellen Nadeau, NIST

ISOAG meets the 1st Wednesday of each month in 2016

ADJOURN

THANK YOU FOR ATTENDING

