

# CSU INFORMATION SECURITY

Presentation for 2012 CSU Auxiliary Conference  
January 11, 2012

# Agenda

- Governance, Risk, and Compliance (GRC) Project
- Virtual Information Security Service Center (VISC)
- Compliance Updates
  - Incident Response – SB 24
  - New CSU HIPAA Portal
- Information Security Updates
- Group Discussion
- Secure IT 2012
- Wrap-up

# **Governance, Risk, and Compliance (GRC) Project**

# GRC Project - Overview

- A GRC System is an ***integrated*** application that offers modules to help automate GRC processes. For example, a GRC system can do the following:
  - Manage policy development, dissemination and attestation
  - Track requirements of law, regulations, standards and security/privacy frameworks
  - Monitor compliance requirements (e.g., PCI and HIPAA)
  - Manage risk assessment activities
  - Track risk mitigation efforts
  - Manage and track incidents

# GRC Project – CSU Requirements

- Single portal that will:
  - Support the CSU organization structure
  - Foster a collaborative environment.
  - Harmonize compliance requirements and controls
  - Support campus-based and third party risk assessments
  - Support campus reporting and governance activities
  - Support incident management requirements

## **GRC Project – CSU Project Timeline**

- Issued RFP on January 6th
- Proposals are due on January 27<sup>th</sup>
- Finalist presentations occur on February 9 & 10
- Contract starts on March 1<sup>st</sup>

# **Virtual Information Security Service Center (VISC)**

# Virtual Information Security Service Center (VISC)

- VISC is a virtual organization comprised of staff resident on multiple CSU campuses that operate under the VISC Governance Committee
- Focuses on security services that are common to all campuses and can be efficiently delivered “virtually”
- VISC operations are overseen by a qualified ISO
- VISC priorities, operational plans, and service levels are approved by a governance group comprised of the CIOs of the participating campuses and the systemwide CISO
- Participating campuses share resources for their mutual benefit including costs

# Virtual Information Security Service Center (VISCC)

- Participating in the VISCC does not replace the need to maintain information security services on the campus.
- Campuses are still responsible for their information security program.
- Campus VISCC liaisons are responsible for communicating with stakeholders (including the President) on their campuses.

# Virtual Information Security Service Center (VISCC)

- VISCC began as a pilot project in March 2010 with seven campuses plus the CO:
  - Bakersfield
  - Channel Islands
  - Dominguez Hills
  - East Bay
  - Fullerton
  - Northridge
  - Monterey Bay
  - Chancellor's Office
- In March 2011, six additional campuses joined the VISCC: Fresno, Humboldt, Maritime Academy, Sacramento, San Francisco, and Sonoma

# Virtual Information Security Service Center (VISCC)

## VISCC services include:

- Standards/Procedures development
  - Develops standards, guidelines, and processes aligned with systemwide IS policies
- System-wide collaboration and communication
  - Serves as liaison with appropriate CO and campus consortiums and committees
- Incident Management and Litigation Hold
  - Aids campuses by gathering information, conducting forensic investigation, and other activities needed to understand the extend of the breach
- Security Awareness Training Program Coordination and Reporting
  - Coordinates the delivery of the SAT program delivered by the CO,
  - Reports on training participation
  - Coordinates the creation of campus user accounts

# Virtual Information Security Service Center (VISC)

## VISC services (continue)...

- Information Security risk assessments
  - Oversees the initiation of the VISC risk assessment procedure
- Vulnerability assessment, scans, and reports
  - Schedules vulnerability scans
  - Performs internal and external PCI scans
  - Reviews current threats and identifies potential risks
- Network and log management
  - Monitor the usage of participating campus networks and systems to detect unauthorized access and potential vulnerabilities
  - Review and assess security logs and system general alerts
  - VISC defines regulatory alert criteria, implements log event management and alerting,
  - Coordinates with the Virtual Network Operation Center (VNOC)

# Virtual Information Security Service Center (VISIC)

## VISIC services (continue)...

- Security Tools and Services
  - Reviews and selects tools, negotiates contracts, and coordinates the purchased for shared software and services.
- Application Service Provider Reviews
  - Coordinates reviews and software purchase requests
- Audit Preparation
  - Assists campuses with audit preparation and responses
- Project Management
  - Undertakes research and development projects – such as review tools, products, and services
- Metrics
  - Develops metrics and reports regarding VISIC delivered services

# Virtual Information Security Service Center (VISIC)

VISIC provides the CSU with a way to manage the growth of information security requirements and costs by pooling expertise and leveraging technology to perform common tasks.

# Compliance Updates

# Incident Response – SB 24

- Amends sections 1798.29 (agency) and 1798.82 (person or business) effective January 1, 2012
- Additional requirements pertaining to security breach notifications:
  - (Req) Breach notice must be written in plain language
  - (Req) Notice must include, at a minimum, the following:
    - Name and contact information of the reporting agency
    - Listing of the types of PI that were or are reasonably believed to have been the subject of the breach
    - If possible, date of the breach, estimated date of the breach, or date range within which the breach occurred
    - Date of the notice
    - Whether the notice was delayed as a result of a law enforcement investigation
    - General description of the breach incident
    - Toll-free telephone numbers and addresses of the major reporting agencies, if the breach exposed a SSN, driver's license number, or CA identification card number
  - (Opt) At the discretion of the agency, the notice may also include:
    - Information about what the agency has done to protect individuals whose information has been breached
    - Advice on steps that the person whose information has been breached may take to protect himself or herself

# Incident Response – SB 24

- Requires agency, person, or business that is required to issue a security breach notice to more than 500 CA residents pursuant to existing law to electronically submit a single sample copy of that security breach notice to the Attorney General
- The law requires that a covered entity under HIPAA is deemed to have complied with the laws provisions, if it has complied with existing federal law.

# HIPAA & HITECH

**The HIPAA Privacy Rule** requires appropriate safeguards to protect the privacy of personal health information (PHI), including individual medical records and sets limits and conditions on the uses and disclosures that may be made of such information. At the CSU, the HIPAA Privacy Rule is enforced by the CSU HIPAA Privacy Official within Human Resources Management (HRM), in the Chancellor's Office.

**CSU HIPAA Privacy Official:**

**Michelle Hamilton**

CSU Office of the Chancellor, Human Resources Management

401 Golden Shore, Long Beach, CA 90802

Phone: (562) 951-4413 or (562) 951-4411

Facsimile: (562) 951-4954

E-mail: [mhamilton@calstate.edu](mailto:mhamilton@calstate.edu)

# HIPAA & HITECH

**The HIPAA Security Rule** requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic PHI (e-PHI). At the CSU, the HIPAA Security Rule is enforced by the Chief Information Security Officer at the Chancellor's Office, who also serves a dual role as the CSU HIPAA Security Official.

**CSU HIPAA Security Official:**

**Cheryl Washington**

CSU Office of the Chancellor, Information Security Office

401 Golden Shore, Long Beach, CA 90802

(562) 951-4190

Facsimile: (562) 477-5951

E-mail: [cwashington@calstate.edu](mailto:cwashington@calstate.edu)

# HIPAA & HITECH

HITECH describes the notification process for disclosure of medical information subject to HIPAA

- If a breach of physical PHI or ePHI occurs, it must be reported immediately upon discovery to the CSU HIPAA Privacy and CSU HIPAA Security Officials **AND** to the campus Information Security Officer (ISO).

The CO's systemwide HR office launched a portal to help campuses with HIPAA and HITECH compliance efforts: [http://www.calstate.edu/hradm/hipaa/HIPAA\\_Portal1.shtml](http://www.calstate.edu/hradm/hipaa/HIPAA_Portal1.shtml)

- Resources available on the portal include:
  - CSU policies
  - CSU HIPAA Privacy Manual
  - CSU Privacy Notice
  - CSU Business Associate Agreement template
  - HIPAA training materials
  - HIPAA Privacy and Security Regulations

## Information Security Updates

- Data Discovery – Subject to funding approval, the CO intends to purchase Identity Finder for data discovery. Additionally, we are looking to obtain favorable pricing for other campuses that would like to use the tool.
- SEIM Project – Collaborating with VISC to identify a SEIM tool
- SAT Project –Investigating the feasibility of using SANs “Secure the Human” training modules to replace (or supplement) the existing SAT course
- ISAC and IAM are working together to update the CSU’s Digital/Electronic Signature Project and develop supporting digital/electronic signature standards
- New information security standards have been added to the ICSUAM site

# **GROUP DISCUSSION**

# Topics for the group discussion

- Password controls
- DR plans
- Encrypting sensitive data
- Compliance with campus policies and standards
- PCI compliance
- User access reviews
- Security related projects
- Challenges
- Ideas

## CISA/Secure IT 2012

- Conference on Information Technology and Network Security
- Hosted by California State University, San Bernardino and the California Community College Chief Information Systems Officers Association collaborative
- March 18-20, 2011 at the Double Tree Hotel at Ontario Airport
- Details about the Call for Proposals for the CISOA/Secure IT 2011 conference on Information Technology and Network Security can be found at <http://www.secureitconf.com>

# QUESTIONS ?

**Contact: Cheryl Washington  
cwashington@calstate.edu**