COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services

UNIVERSITY OF CALIFORNIA

Audit Compliance Investigations Presidential Policies Contact

This Issue's Contents

Cybersecurity

A Rational Approach to Cybersecurity: An Introduction to the NIST Cybersecurity Framework

How does UC effectively approach cybersecurity given all the challenges and resource constraints involved in the increase of cyber-related breaches across the U.S. announced daily in the media? The answer is through adopting an approach that organizes our efforts around the key functions necessary to address cyber risks and prioritizes our efforts to ensure this is done in a cost-effective way based on the needs of the University. One approach to achieve this is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

The NIST CSF was created by the federal government as a result of a Presidential Executive Order to improve critical infrastructure cybersecurity and was completed and released in February 2014. Since that time it has been increasingly adopted by organizations to inform their approach to addressing cybersecurity risks. The framework is not a checklist of things to do to address cybersecurity, but rather is a risk-based approach that focuses on business needs and considering cybersecurity risks as part of the overall risk management process. At the heart of this framework are the five core functions used to organize and express how an organization is addressing its management of cybersecurity risk. These functions are Identify, Protect, Detect, Respond, and Recover.

Associated with the functions are specific cybersecurity outcomes called categories that are tied to the programmatic needs and activities that support the function. These are further defined by sub-categories and informative references, which can be aligned with various standards, guidelines, and practices. This includes

Here's What's Happening at ECAS

- UC Global Operations (UC GO) is a new website to connect UC faculty, staff, students, and foreign collaborators with the information they need to navigate the complex world of international activities. The site is currently being reviewed, with a wide release date set for September 2016.
- Sexual Violence and Sexual Assault Education and Training Updates:
  - Undergraduate and Graduate Students will have a revised online training module available in Fall 2016.
  - Online training module for staff and faculty will be translated into three languages: Spanish, Mandarin, and Tagalog. Estimated roll out date is Fall 2016.
  - The services of an onsite live theater performance group (Life Theatre) will be made available for additional employee training to all locations (10 campuses, LBNL, and UCOP).
- Sexual Harassment Prevention Training Webinar Series: ECAS will be working with campus partners to develop and produce a series of live webinars for the academic year on a variety of topics including UC SVSH Policy, Responsible Employer, and Prevention.
- Presidential Policies In The Works:
  - Clery
  - Video Surveillance
- Ethics and Compliance Training
  - Conflict of Interest online course update to be rolled out in the Fall.
  - General Ethics and Compliance Briefing online course update to be rolled out in the Fall.
- Cybersecurity Awareness Training is undergoing revisions in its second year of implementation. New content includes interactive modules as well as a refresher course for those who received standard online training the previous year.

resources such as ISACA COBIT, ISO standards, and other NIST special publications. Together, the supporting categories, subcategories, and informative references help an organization achieve the key functions to addressing cybersecurity.

The functions are defined by NIST as:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The NIST CSF also provides an approach for deciding which controls are necessary and how they should be implemented. The approach to assess the current state of cybersecurity efforts in each of these functional areas uses the framework to map current cybersecurity efforts to the framework core. The outcome of this effort is the creation of a “Current Profile” of the organizations cybersecurity efforts. This can be used as a starting point to assess if cybersecurity efforts are adequate given the risk tolerance of the organization or if improvements are needed, can be used as a starting point to develop an action plan to achieve the desired outcome, or “Target Profile.”

Currently here at UC, we are moving forward with an initiative to assess the general current state of cybersecurity at each location utilizing the NIST CSF. Through this assessment process we will be creating an initial baseline profile to inform the development of a target profile describing where we want to go as an organization based on the NIST CSF framework. This initial baseline review is scheduled to be completed in early 2017.

More information on the NIST Cybersecurity Framework can be found here: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Investigations

Coming Soon: Campus Title IX Investigation Support

The Office of Ethics, Compliance & Audit Services investigations unit is expanding. We are currently interviewing candidates to fill two newly created positions as Sexual Violence/Sexual Assault Principal Investigators. These investigators will be available to support UC Title IX offices system-wide for overflow cases and matters that best lend themselves to non-campus investigators. The new investigators will also be available for Whistleblower complaints and other matters traditionally handled out of this office. We look forward to providing more robust support to your individual locations. We anticipate that these positions will be filled during Fall 2016. Please direct inquiries to the system-wide Director of Investigations: will.mallari@ucop.edu.

Meet the Current ECAS Investigations Staff

LeVale Simpson re-joins the UC Office of the President after most recently serving at the UC Berkeley campus as Staff Investigator (in which he investigated complaints of Improper Governmental Activity, including retaliation, discrimination, and harassment) and as interim Public Records Coordinator in the Office of Ethics, Risk, and Compliance Services. Prior to Berkeley, LeVale previously served as a Residence Analyst in the Office of the General Counsel at UCOP.

Mike Sandulak brings his extensive legal, investigative, and law enforcement experience to the recently created position of Health Sciences Investigator. Mike joined us from UC San Diego where he most recently conducted Title IX investigations and responded to other bias, harassment, and discrimination complaints. Prior to joining the University, Mike was an FBI Special Agent where he investigated a broad range of federal crimes, including health care fraud, cyber and internet crimes, and public corruption.

Judith Rosenberg has been a Principal Investigator with ECAS since 2011. She has conducted investigations related to complaints of Whistleblower Retaliation, discrimination, harassment and management concerns, and provided training at the UC campuses and Lawrence Berkeley Lab. Prior to coming to UC, Judith was the Court appointed monitor for a Federal Class Action involving complaints of sexual harassment and retaliation in the U.S. Forest Service and a case involving rights of disabled prisoners in California.

Will Mallari joined ECAS as the system-wide Director of Investigations in December 2015. Will brings years of experience planning, conducting, and directing complex investigations as an attorney, workplace investigator, criminal investigator, and

University of California administrator. Will previously oversaw and conducted investigations, including Title IX, at UC Berkeley and UC San Diego. Before joining the University, Will worked as a labor and employment attorney, workplace investigator, a police officer, and crime scene investigator.

Clery

Analysis and Recommendation Regarding Clery Handbook Update and CSA's

The Department of Education (DOE) recently updated the Clery Handbook in June 2016, offering clarification on several areas including characterizations of Campus Security Authorities (CSA's). It is important to note that the Clery Handbook is not binding on institutions as it is not a Federal Act or regulation. Instead, it is intended to be an illustrative tool which represents the DOE's interpretation of the Higher Education Act to assist campuses as they navigate the challenges presented with Clery compliance.

The updated Handbook set forth expanded examples of which campus functions should be designated as CSA's. The University of California recognizes the important value of providing survivors of sexual assault and visitors to the ombuds office with confidential resources to encourage reporting of wrongdoing and achieving conflict resolution.

Accordingly, UC will maintain the confidential nature of the ombuds office and victim advocates and continue its current practice of NOT designating them as CSA's. Essential Clery information will continue to be reported by other campus resources who are CSA's.

Health Science Compliance

New OCR HIPAA Audits

In an effort to assess compliance with HIPAA Privacy, Security and Breach Notification rules, the Office for Civil Rights will begin its second phase of audits. Covered entities and business associates selected for phase two received notification letters on July 11, 2016. Audits are expected to commence in the fall.

OCR News Releases

HIPAA penalties, privacy and security breaches are resulting in huge fines for medical centers and hospitals (including academic medical centers). Recently, three major penalty announcements added up to $10.95 million in fines.

- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million – August 4, 2016
- Multiple Alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC) – July 21, 2016
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016

Human Resources

Actions Needed to Improve Clarity and Address Differences Across Federal Data Collection Efforts

After conducting a study analyzing the different federal agencies that collect data on sexual violence, the U.S. Government Accountability Office is recommending standardization of sexual violence data definitions and collection.

Research Compliance

New UC Center of Excellence in Field Research

Sara Souza, Research Safety Specialist at UC Berkeley's Office of Environment, Health & Safety, began her role of leading the new UC system-wide Center of Excellence (CoE) in Field Research Safety on July 1.

The CoE Field Safety Center will support development of field safety plans and promote sharing of best practices in field research. One of the key initial CoE projects is development of a UC Field Safety Operations Manual and corresponding website.

In the meanwhile, please feel free to review the recent Safety Spotlight poster "5 Suggestions for Field Researchers" or refer field researchers and trip leaders directly to Sara at 510-643-5809 or sarasouza@berkeley.edu.

For more information about the UC Centers of Excellence program, please visit the UCOP CoE website.

New NIH Policy Requiring the use of a Single IRB for Multi-site Research Studies

To accelerate the conduct of multi-site clinical research studies, the National Institutes of Health has issued a new policy requiring all multi-site studies involving the same protocol to use a single IRB to carry out the ethical review of the proposed research. Time to review and approve studies at multiple research sites has long been a concern; with this new policy, the NIH seeks to end duplicative reviews that slow the start of the

research. The sIRB policy applies to all competing grant applications (new, renewal, revision, or resubmission) with receipt dates on or after May 25, 2017, all contract solicitations issued on or after May 25, 2017, and all NIH Intramural Studies submitted for initial IRB review after May 25, 2017.

NIH has released guidance, a model authorization agreement, and a model communication plan for institutions impacted by this new policy. Of particular importance is the guidance on direct and indirect cost charges allowed under the new policy. UC already has in place a reliance agreement between its campus IRB's, allowing for single IRB review for multi-site studies. Contact your campus IRB office for information about the use of the UC MOU for Human Research Protections at University of California campuses and Lawrence Berkeley Lab.

Additional Resources:

1. Single IRB FAQs
2. Direct and Indirect Costs under the NIH single IRB policy
3. UC MOU for IRB Review of Human Subjects Research

UCR's Inaugural Export Control Awareness Day

On Friday, June 3rd, UCR held an Export Control Awareness Day that was sponsored by Research and Economic Development (RED), Office of International Affairs (OIA), and Campus Ethics and Compliance Office (CECO), with support from ECAS.

Concurrent seminars were presented across campus to increase individual and institutional awareness of U.S. Export Control laws and regulations. Heightened National Security concerns around access to sensitive technology and information, at a time when international exposure and collaboration is increasing – the U.S. State, Commerce and Treasury Departments are paying closer attention to export compliance at universities. Recent government enforcement activities at various universities have resulted in a number of audit findings with civil and criminal liability consequences, including monetary penalties and imprisonment.

The goal was for the UCR community to know when Export Control laws and regulations apply, who to contact, and how to prevent institutional and personal liability and violations.

Separate presentations and workshops were broken down for Faculty and Researchers, Administrative Staff, Sponsored Programs and Tech Transfer, Business Contracts & Finance and Material Management.

Policy

UC Policy Process

The University Policy Office oversees the policy-making process for the University of California in all areas for which the President has authority. Policy approval process flow charts are now available for further guidance:

- UC Presidential Policy Process—Existing Policies
- UC Presidential Policy Process—New Policies

New UC Policies

UC Health Participation in Activities under the End of Life Option Act:

Interim policy effective 6/9/16.

Recent UC Policy Updates

PPSM-64 Termination and Job Abandonment:

Effective 7/15/16, policy revisions include incorporation of PPSM-65 and PPSM-67, added job abandonment section, and added references to non-Roman numeral salary grades and classifications in use for MSP employees.

PPSM-1 General Provisions:

Effective 7/14/16, policy has undergone technical revisions.

PPSM-2 Definition of Terms:

Effective 7/14/16, policy revisions include added definitions, removed definitions and references, and the rescindment of PPSM-2 dated 9/1/2009.

PPSM-70 Complaint Resolution:

Effective 7/14/16, policy revisions include incorporation into policy PPSM-71, added references, alignment with revisions to Policy on Sexual Violence and Sexual Harassment, and added sections.

PPSM-82 Conflict of Interest:

Effective 7/14/16, technical revisions were made to this policy in February 2016, including updates to web and document links, office titles, updates to named employees, and typographical amendments.

Self-Supporting Graduate Professional Degree Programs:

Effective 7/12/16, policy revises and supersedes the September 23, 2011 policy and guidelines.

Privacy

Protecting Privacy in Genomic Databases

The use of databases to contain people's medical histories for genomic studies carries various privacy risks. In order to reduce the chance of it being compromised, researchers from MIT and Indiana University at Bloomington have developed a new system that allows databases for genome-wide association studies to be used, but reduces privacy concerns to nearly zero.

Despite Expectations of Privacy, One in Four Share Sexts, Study Finds

A study conducted by Indiana University has found that approximately 23 percent of sexts (suggestive text messages) are shared. This is despite the sentiment of 73 percent of senders who would feel discomfort if the intended receiver shared their private messages with others.

Your Internet Privacy Should Be Up For Sale

The Federal Communications Commission has recently proposed further regulations meant to better inform consumers of how companies monitor their online activities. In addition, the FCC is looking to further curb the rising market in internet privacy, such as pay-for-privacy plans.

Ctrl+Z: The Right to be Forgotten

The European Union Data Protection Regulation, adopted in April 2016, aims to regulate online data privacy by providing citizens with the ability to eliminate their digital trace. Data companies, such as Google, would have the legal duty to delete information user's believe infringe on their rights.

Upcoming Educational Opportunities

- October 17-18—Clinical Research Billing Boot Camp (Irvine)
- October 21—UC Merced Staff Hiring Process (Webinar)
- October 31-November 1—Clinical Research Billing Boot Camp (Oakland)
- November 1—UC New Auditors Orientation (Oakland)
- TBA—2017 Compliance Symposium