THE UW TACOMA FIRST ANNUAL CYBERSECURITY CAPSTONE CHALLENGE
DECEMBER 7, 2013

UNIVERSITY OF WASHINGTON TACOMA

PROFESSIONAL PROFILES AND CYBERSECURITY CHALLENGES

INSTITUTE OF TECHNOLOGY UNIVERSITY OF WASHINGTON | TACOMA

MILGARD SCHOOL OF BUSINESS
# Table of Contents

**Agenda**
- Kristine’ Reeves Bio .................................................. 3

**Cybersecurity Challengers**
- Continuant ............................................................. 5
- Internet Identity ......................................................... 7
- MK Hamilton Associates ............................................ 8
- Microsoft Challenge A ............................................. 9
- Microsoft Challenge B ............................................. 11
- Pierce County ......................................................... 13
- Port of Tacoma ......................................................... 16
- Tacoma Power ......................................................... 18
Welcome by Dr. Goda……………………………………………………………………………5:00 PM
Keynote, Mrs. Kristine’ Reeves…………………………………………………………………5:15 PM
Dinner ..................................................................................................................................5:30 PM
Table Rotation – Meet the Challengers.........................................................................5:30 – 7:00 PM

KRISTINÉ M. REEVES
BIOGRAPHY
Director of Military Sector Development

Kristiné Reeves, a Washington state native, currently serves as the Director of Military Sector Development in the Office of Economic Development and Competitiveness for the Washington State Department of Commerce, based in Seattle.

Prior to joining the Department of Commerce, over the past five years, Reeves served as the Kitsap & Olympic Peninsula Director, the South Sound Regional Director and the Statewide Veterans Constituency Coordinator for U.S. Senator Patty Murray.

During her time with the Senator, Reeves was instrumental in facilitating a Senate Veterans Affairs Field Hearing in Tacoma, increasing networking and relationship development with the Navy and the Army, and worked intimately on military transition and workforce development issues in the state.

Prior to joining Murray’s staff, Reeves worked for the Community Colleges of Spokane as an Immigration Compliance officer in International Programs and served the Eastern Washington community in a variety of different non-profit positions. Reeves has nearly ten years of experience in higher education related to international programs, cultural and diversity programs and over fifteen years of community service and civic engagement advocacy work.

Passionate about servant leadership, public participation in the political process and education; Reeves spends time outside her work volunteering in the community with her Sorority, Zeta Phi Beta, and participating in various charitable organizations, including the Urban League, March of Dimes, the American Cancer Society, the National Education Foundation and more.

Reeves received her bachelor’s degree in political science from Washington State University-Pullman and her master’s degree in Organizational Leadership from Gonzaga University. She is currently a year into her PhD in Public Policy and Administration. Reeves currently spends her time away from the office with her husband, Camron, her one year old son James, and her large family in Eastern Washington.
2013- 2014
Corporate and Government
Cybersecurity Challenges
Name of Continuant’s Cybersecurity Challenge

Unified Communication Cybersecurity Vulnerabilities and Mitigation

Point of Contact Information

Mr. Mike Hanks, MikeHa@Continuant.com, 253.252.3156

Company Profile

Continuant has a proven track record of leadership in delivering comprehensive maintenance solutions for enterprise communications systems. Initially offering installation and support services for traditional key and PBX systems, Continuant has expanded to address customer needs in other markets such as Unified Messaging and VoIP. As the network quickly evolved to become the backbone of company communications, and traditional voice and data became Unified Communications (UC), Continuant developed new technologies and service offerings to fulfill the needs of our customers. Continuant is unique in that we provide customers with the power of choice, providing an unbiased consultation and certified support for equipment from most of the major communication technology manufacturers, such as Cisco, Avaya, Nortel and Siemens. Our balanced approach to continuity maximizes uptime, reduces operating expenses, and provides every customer with a single point of contact.

Continuant Challenge Description

Continuant personnel use a variety of UC solutions designed primarily from components of leading communication systems such as Avaya, Cisco, and Microsoft. These UC solutions allow Continuant to communicate through modalities of messaging, voice, and conferencing (audio, video, and web) as an integrated set of capabilities through common desktop and mobile clients. Security threats in the UC environment are just as important to an enterprise as traditional IP and data network-based threats. A cybersecurity attack on an exposed UC environment could severely damage an enterprise. These security threats may include telephony denial of service (TDos), modems, and toll fraud (outsider dial-through access).

The proposed Cybersecurity challenge is to conduct a vulnerability assessment on Continuant’s corporate UC environment. The vulnerability assessment may include UC component compliance against the National Vulnerability Database (NVD). Time permitting, additional manufacturer components may be tested within Continuant’s lab environment. Students will be asked to present their findings, along with recommendations on mitigation techniques. Continuant corporate UC environment* includes access to the following equipment:

- Enterprise Voice Telephony
- Cisco Unified Communication Manager Release 8.6
- MCS78xx servers, Linux OS
- Conferencing
- Cisco Meeting Place – 8
- Cisco WebEx
• Microsoft Lync 2010
• Messaging
• Microsoft Exchange Server 2010
• Unified Messaging
• M & Presence
• Microsoft Lync 2010
• Clients
• Cisco 7942, 7962, 7937 & 7965 Desk Phones
• Cisco Soft Phones
• Apple iPhones 3, 4, & 5 (Through ActiveSync)
• Various webcams

We believe the Continuant environment will coincide with the UWT MCL vision of serving as an educational foundation for invention, innovation and entrepreneurship. The graduate students will enhance the learning of necessary skills to advance in Cybersecurity operations.

Site Location
Continuant’s corporate headquarters is located at:
Continuant, Inc.
5050 20th Street E
Fife, WA 98424

Continuant is a local and viable option to UWT students who wish to learn at a company with a proven track record of leadership, in delivering comprehensive maintenance solutions.

Expected Timeline
Jan-May 2014
Name of Internet Identity’s Cybersecurity Challenge
Network Security Assessment inside the Cyberthreat Lab: Real World Approaches in a hostile environment

Points of Contact Information
Merike Kaeo, merike.kaeo@internetidentity.com, 253.590.4100 x8002
Chris Richardson, chris.richardson@internetidentity.com, .253.590.4100 x4090

Company Profile
Internet threats are constantly evolving and becoming more complex. In order to stay one step ahead of nimble bad actors, organizations must form a broader, more structured, trusted information-sharing network.

The ActiveTrust network by IID enables trusted threat intelligence collaboration for enterprises and governments. The company aggregates widely sourced threat data and delivers actionable intelligence to enable the protection of users, brands and business growth.

IID’s ActiveTrust platform enables threat intelligence sharing in a trusted environment that reaches beyond limited trust groups. ActiveTrust delivers automated threat intelligence that allows network members to maximize their most valuable resources, human capital and time, and focus on their core business.

Top financial firms, the largest government agencies, and leading e-commerce companies, social networks and Internet service providers leverage IID to detect and mitigate threats.

Description of Your Challenge
A controlled assessment inside our Threat Intelligence Lab on current approaches, and what unique challenges and solutions are presented in an environment like this.

A potential phase 2 could be the larger implications of a network defense team in a large organization having to craft special security exceptions to the conventional operating rules and safeguards in order to test various security measures and see new threats at the edge.

Site Location
1142 Broadway, Ste 400
Tacoma, WA 98401

Expected Timeline
We can discuss.

Desired skill sets within the team
Policy documentation, testing, analysis, plan documentation, and whatever else we can come up with.
Name of your Challenge
Developing security consulting skills

Point of Contact Information
Michael Hamilton; mkh@mkhamiltonassociates.com

Company Profile
MK Hamilton and Associates was formed by Michael Hamilton, former Chief Information Security Officer for the City of Seattle; former Vice-Chair and now cybersecurity subject matter expert for the State, Local, Tribal and Territorial Government Coordinating Council, and former Managing Consultant for VeriSign Global Security Consulting. Mike’s business partners include the former Director of Emergency Response for King County; a Vice President of HR for T-Mobile; and a former Director of International Business Consulting for technical product sales.

We are a start-up located in the City of Bremerton, within walking distance from the ferry terminal and Puget Sound Naval Shipyard. Our business execution is in four areas: cybersecurity consulting, product sales, managed security services and talent acquisition. Our market is state, local, tribal and territorial governments, 911 operation centers, public utility and other special purpose districts. We secure the infrastructure that provides life-safety, life-sustaining and quality of life services at the scale most important to the American way of life.

Description of Your Challenge
We will deploy students along with seasoned professionals, in order to mentor the students in the execution of information security consulting roles. Depending on the qualifications of the students, this may be primarily technical (e.g. vulnerability assessment, penetration testing); more consultative (risk assessment, compliance consulting); security project management; or a focus on the sales process and relationship management.

Students will learn consulting “soft” skills, the use of technical assessment tools, the process of risk analysis, deliverable preparation, and how to leverage technical skills as part of the sales process. Students will be exposed to multiple commercial technologies (FireEye, Snort, Barracuda) as well as open-source security monitoring solutions. Students will learn the lexicon of compliance, for regulatory requirements that may include NERC-CIP, CJIS, HIPAA, or PCI.

Site Location
Work will be based in Bremerton, but students may work remotely as needed.

Expected Timeline
We expect to take students through at least one fiscal quarter of company operation.

Desired skill sets within the team
Skills desired are technical, including the use of technical security assessment tools (although we can train them); “people” skills (speaking, writing), and a basic knowledge of information security standards of practice and regulatory requirements.
Name of Microsoft’s Challenge A

Business impact of security: How to Quantify Business value

Point of Contact Information

Jackson Robinson jacksro@microsoft.com 425.421.7455

Company Profile

Microsoft IT is for those IT professionals and business technology professionals who want to be strategic partners to the business and be the first place to create innovative solutions using all of Microsoft’s products and services. Microsoft IT provides career growth opportunities, a rewarding and flexible work environment so you can better integrate professional and personal life. Inspiring what’s next, Microsoft IT employees make global impact on thousands of customers and thousands of employees who use Microsoft software and services.

Information Security and Risk Management (ISRM) is an organization within Microsoft IT that is responsible for the data protection of Microsoft assets, business and enterprise. ISRM’s vision is to ensure all information and services are protected, secured, and available for appropriate use through innovation and a robust risk framework


Microsoft Challenge Description

A key challenge to a non-revenue organization in any company is how you demonstrate value from security activities. This challenge will require extensive research and understating the Microsoft LOB development environment to describe an approach to create a solid story for embedding security in application development. This goes beyond current Security Development Lifecycle activities. It will need to show security value to application and infrastructure teams. Culmination of the project will lead to recommendations of how to build a value enabled case for security within IT. The lack of a tangible product or increased feature set keeps security planning and funding to minimum for most applications. Microsoft is looking to streamline and update the story to internal process units (HR, Finance, etc).

Areas to be addressed

How to increase security investment and demonstrate value to businesses?  
How do you move security planning from an afterthought as a value proposition?  
How do you build business cases for proactive security initiatives to enhance features and timelines?  
Drive recommendations beyond simple bug counts and create solid metrics for quantifying security value.
Deliverables

1. Comprehensive report
2. Executive overview
3. Present finding to mock leadership board

Site Location

18600 Union Hill Road
REDMOND, WA
98052, United States

Expected Timeline

TBD by team

Desired skill sets within the team

These are the key skills (Be)

Excellent written, verbal and presentation skills are required
Strong analytical and organizational skills are essential and required

Must be able to work autonomously as well as in team environments, often in stressful, high impact situations

When added with technology (Know)

Knowledge of Application Security Principles and Guidelines.
Knowledge of Basic operational and infrastructure security principles and guidelines a huge plus.
Allows people to do these tasks (Do)

Work with internal customers to understand their business portfolio and inject appropriate security control to enable a secure posture for the portfolio.

Experience in consulting/advisory capacity driving security controls into solution development.
Name of Microsoft’s Challenge B

Security guidance for cutting edge technologies for SQL DAP (Database auditing and Protection) or Power BI

Point of Contact Information

Jackson Robinson jacksro@microsoft.com 425.421.7455
Yale Li Yuhang.Li@microsoft.com

Company Profile

Microsoft IT is for those IT professionals and business technology professionals who want to be strategic partners to the business and be the first place to create innovative solutions using all of Microsoft’s products and services. Microsoft IT provides career growth opportunities, a rewarding and flexible work environment so you can better integrate professional and personal life. Inspiring what’s next, Microsoft IT employees make global impact on thousands of customers and thousands of employees who use Microsoft software and services. Information Security and Risk Management (ISRM) is an organization within Microsoft IT that is responsible for the data protection of Microsoft assets, business and enterprise. ISRM’s vision is to ensure all information and services are protected, secured, and available for appropriate use through innovation and a robust risk framework


Microsoft Challenge Description

Create industry security guidance by developing technical content with our SAFE-T (Security Accelerators for Emerging Technology) Team. The team routinely writes guidance on emerging technologies at Microsoft. We currently have two topics that need to be completed by the end of June.

1. Security guidance on Power BI – This product is days away from public release.

   a. What is Power BI: “It’s easier than ever to transform complex data into meaningful insights and share them with your team. Power BI for Office 365 is a powerful new way to visualize and interact with data in Excel and Office 365. Search, discover, and with just a few clicks, analyze, shape, and transform your data into stunning interactive visualizations that uncover hidden insights. Work, collaborate, and share from anywhere, on any device with Power BI for Office 365.”

   b. As tools become easier for both technical and non-technical teams to access security must focus on how we protect data. The document needs to cover casual user to programming interfaces.


2. Security guidance on SQL DAP (Database auditing and Protection)

   a. Dap as defined by Gartner, “Database audit and protection (DAP) tools provide comprehensive security for relational database management systems (RDBMSs). DAP tools have their roots in the basic monitoring capabilities of database activity monitoring (DAM) tools. In response to expanded client requirements, vendors have added additional capabilities, such as data discovery and classification, threat and vulnerability management, application-level analysis, intrusion prevention and activity blocking, and identity and access management analysis.” http://www.gartner.com/it-glossary/database-audit-and-protection-dap/
b. This Challenge will require teams to look what DAP is and how to implement it in SQL. Taking solid principles and implementing them within the Microsoft stack.

Creating the guidance is the primary goal of this project, the stretch goal is to work with our TechNet team to publish the guidance. The core content is the most important however student can get public authoring credit if the work is substantial enough for publication.

**Deliverables**

1. Comprehensive article intended for publication
   a. Security guidance
      i. Hardware level
      ii. Configuration and installation
      iii. Code samples (optional)
      iv. Policy
      v. Best practices
   b. Stretch goal is publication on Microsoft TechNet

2. Present approach to technical audience

**Site Location**

Redmond with remote synch-ups
18600 Union Hill Road, REDMOND, WA  98052, United States

**Expected Timeline**

TBD by team

**Desired skill sets within the team**

**IT professional skills.**

- Must understand server installation and configuration.
- Able to read and understand TechNet articles.

**Optional skills**

- Programming is helpful for MSDN publication of coding samples.
- Math or statistical background for big data analysis would be beneficial.
Name of Pierce County’s Information Technology Department’s Challenge

Critical Security Control Audit

Point of Contact
Linda Gerull (253) 798-7476 lgerull@co.pierce.wa.us
Director, Information Technology

Company Profile Pierce County is committed to advancing cybersecurity best practices that will protect government systems from intrusion or data theft. Taxpayers expect government to secure their information and we are committed to fortifying our infrastructure in this ever-changing technology landscape. The proposed project, Critical Security Control Audit will give us new insights and transparency in our security efforts. The Audit can also be applied to other agencies and companies.

What will make the Pierce County project so complex, interesting and educational for students? Pierce County IT supports: e-commerce, mobile applications, court management systems, integrated networks, external subscribers to county systems, commercial devices, SAAS providers, public wifi, and a large number of interactive web-based public services. Pierce County IT supports 24 different business units from public works to juvenile justice. No other organization has the range of business systems and system complexity.

Pierce County’s Challenge Description
The Critical Security Controls standards Version 4.1 adopted by the Department of Defense, the State Department and foreign countries, describes 20 areas of system and network security that should be implemented. These controls are best practices and includes a “check list or recipe” of how to evaluate an organizations systems. The scope of the Critical Security Control Audit is to evaluate the extent to which Pierce County is adhering to or implementing the Critical Security Controls and prepare a report, documentation, and recommended procedures to improve implementation. The UWT project team in conjunction with the Pierce County team will select 3-5 Critical Security Control areas to evaluate. These areas are:

20 Critical Security Controls - Version 4.1

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response and Management
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

For each of the Critical Controls the UWT team will assess the County's compliance with the recommendations for the Control. The Control recommendations are defined as Quick wins to Advanced. For example the following is the list of criteria for Malware Defenses:

1. Quick wins: Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. The endpoint security solution should include zero-day protection such as network behavioral heuristics.

2. Quick wins: Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update.

3. Quick wins: Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media. If the devices are not required for business use, they should be disabled.

4. Quick wins: Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

5. Quick wins: Scan and block all e-mail attachments entering the organization’s e-mail gateway if they contain malicious code or file types unneeded for the organization’s business. This scanning should be done before the e-mail is placed in the user’s inbox. This includes e-mail content filtering and web content filtering.

6. Quick wins: Apply anti-virus scanning at the Web Proxy gateway. Content filtering for file-types should be applied at the perimeter.

7. Quick wins: Deploy features and toolkits such as Data Execution Prevention (DEP) and Enhanced Mitigation Experience Toolkit (EMET), products that provide sandboxing (e.g., run browsers in a Virtual Machine), and other techniques that prevent malware exploitation.

8. Quick wins: Limit use of external devices to those that have a business need. Monitor for use and attempted use of external dev Visibility/Attribution: Block access to external e-mail systems, instant messaging services, and other social media tools.

10. Visibility/Attribution: Ensure that automated monitoring tools use behavior-based anomaly detection to complement and enhance traditional signature-based detection.
11. Visibility/Attribution: Utilize network-based anti-malware tools to analyze all inbound traffic and filter out malicious content before it arrives at the endpoint.

12. Advanced: Perform continuous monitoring on all inbound and outbound traffic. Any large transfers of data or unauthorized traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.

13. Advanced: Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running undetected on corporate systems. Samples should be provided to the security vendor for “out-of-band” signature creation and deployed to the enterprise by system administrators.


15. Advanced: Deploy “reputation-based technologies” on all endpoint devices to cover the gap of signature-based technologies.

16. Advanced: Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

17. Advanced: Apply proxy technology to all communication between internal network and the Internet.

Final Deliverables
The UWT team will complete a document that summarizes the evaluation, analysis, compliance and recommendations in 3-5 control areas and present the results to Pierce County IT management. The results should be easy to use and be formulated as an audit (County can provide the format). Each team member will take part in the presentation.

Term of Project
1. All work is the property of Pierce County.
2. UWT may use portions of the project that do not disclose County security or network architectures.
3. UWT team members are asked to keep County security and network information confidential. Any county diagrams or system information shall not leave the County offices.
4. UWT team will be able to work on site with County staff.
5. County will provide work space for UWT team.
6. County will not provide equipment for UWT team.
7. County will not compensation UWT for the work or project results.
8. The County takes responsibility to implementing or not implementing the recommendations and UWT has no liability to the County for this work.
Name of Port of Tacoma’s Cybersecurity Challenge
Port of Tacoma Cybersecurity Program Development

Point of Contact
Martyn Adamson  253.428.8648- madamson@portoftacoma.com

Company Profile
The Port of Tacoma was created by Pierce County citizens in 1918, and considered an economic-engine of Pierce County. It is an independent municipal corporation operating under Title 53 of the Revised Code of Washington, the Port is a special purpose local Government. The Port of Tacoma is one of the largest container ports in North America and one of the top 50 in the world. It is a major center for container cargo, bulk, breakbulk, autos and heavy-lift cargo and designated as a strategic military port for transport of military cargoes.

Presidential Executive Order 13636 issued February 12, 2013 - Improving Critical Infrastructure Cybersecurity called for the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework. Preliminary NIST Cybersecurity Framework is currently available for review and comment.American Association of Port Authorities (AAPA) IT Committee submitted review comments and finalized Cybersecurity Framework expected in February 2014.

As a strategically important commercial and military Port, Port of Tacoma constitutes Critical Infrastructure

Port of Tacoma Challenge Description
Port of Tacoma intends to harden its Cybersecurity position by developing a Cybersecurity Program based on the NIST Framework. Student project is to develop this Cybersecurity Program and associated implementation plans. Cybersecurity Program is intended to be both Strategic, defining a Cybersecurity and risk management structure, and Operational to help identify and prioritize actions for reducing Cybersecurity risk. Program will be developed in coordination with Port of Tacoma Information Technology staff and other stakeholders.

Program is expected to draw heavily from the NIST Cybersecurity Framework, a risk-based approach composed of three parts: Framework Core, Framework Profile, and Framework Implementation Tiers:

Framework Core: Consists of five Functions - Identify, Protect, Detect,

1. Respond, Recover which can provide a strategic view of an organization’s management of Cybersecurity risk
2. Framework Profiles: Identifies opportunities for improving Cybersecurity by comparing a “Current” Profile with a “Target” Profile
3. Framework Tiers: Describe the degree to which Cybersecurity risk management practices exhibit risk and threat awareness and are repeatable and adaptive

During development of the Cybersecurity Program, interaction and consultation with other agencies is anticipated, including:
Port of Tacoma Information Technology Staff
Port of Tacoma Security and Port Patrol
Washington State Fusion Center (WSFC)
PRISEM - Public Regional Information Security Event Management
United States Coast Guard Cyber Command (Department of Homeland Security, sector specific responsibility for Port’s)
**Project Deliverables**  Project plan; periodic status reports

**Cybersecurity Program Recommendations and Implementation Plan** documenting a prioritized and phased approach to program execution and adoption

**Strategic Components:**

**Operational Components**

- Prioritized tasks to be undertaken to meet the Port’s Cybersecurity requirements; an implementation plan
- Scope language defined Cybersecurity and risk management program based primarily on the NIST Core, Profile, and Implementation Tiers Framework
- Scope of language for a Request for Proposal (RFP) to be issued by the Port for services to undertake the first phase (at a minimum) of the implementation plan
Name of Tacoma Public Utilities’ Challenge
UT Maturity Model Framework Policy Creation, Mapping, and Maturity Assessment

Point of Contact Information
Scott Klauminzer, TPU Cybersecurity Lead, (253)-779-7740.sklauminzer@cityoftacoma.org

Company Profile
Tacoma Public Utilities is a publicly owned utility that is owned by the citizens of Tacoma. It is comprised of three divisions – Tacoma Power, Tacoma Water, and Tacoma Rail. Together these divisions make up the largest department in the Tacoma City government. Tacoma Public Utilities is directed by five citizen board directors appointed by the Tacoma city council and operates entirely from revenues from sales of services, not taxes. We believe and are committed to serving our customers, respecting people, caring for our community and environment, achieving excellence and operating safely. Tacoma Public Utilities aims to provide competitive, environmentally responsible electric, water and rail services through teamwork, technology and innovation.

Tacoma Public Utilities Challenge Description
Tacoma Power has recently completed work on a Utility Technology Maturity Model Framework which establishes common practices to describe a mature utility technology delivery organization. The next step is to establish a policy framework and deliver Policy, Standard, and Plan level documentation across TPU surrounding each of the domains of the Framework, focusing initially on 6 foundational domains. In conjunction with the Policy effort, we are to assess our current maturity level against the UTMM Framework, to establish our current maturity, which will aid us in defining future maturity goals. Additionally, at a national level, NIST has been tasked with creating a Cybersecurity Framework for Critical Infrastructure. Our effort will be to map the UTMM Cybersecurity Domains, based on the Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) into the NIST Cybersecurity Framework, and assess a maturity level within the NIST Framework.

Site Location
TPU Main Campus at 3628 South 35th St., Tacoma, WA 98408

Expected Timeline

Desired skill sets within the team
Analytical and documentation skills are a must. Additionally, an understanding of at least one of the following Information Security Frameworks/Control Sets, ISO 27000, Cobit5, ISA99, NIST SP 800-53, ES-C2M2, SANS CSC.