OFFICE OF CYBER DEFENSE COORDINATION

AAKIN PATEL DIANNE HAIGNEY EVERETT WILSON

BEFORE WE START…

Please interrupt me!

If you have any questions, please raise your hand or just speak up! I prefer to discuss as we go along.

I come from a technical background, so sometimes I inadvertently use terminology that not everyone may know. Please ask, and I will clear it up! I like that better than me babbling without anyone understanding what I am saying ☺

THE OCDC

- Who are we?

We are the sole inter-agency cybersecurity resource for entities within the State of Nevada.

- Mission

  To fulfill the tasks and duties set to us via the NRS 480.900-480.950, which is to provide cybersecurity resources, knowledge, assistance, and coordination across all SLTT (State, Local, Tribal, and Territory), infrastructure, and educational entities, and all private entities that wish to participate.

THE OCDC

Guiding Principles

- Help identifying the areas of concern within IT infrastructure across all entities statewide
- Help identifying and eliminating cybersecurity threats in both public and private sectors
- Creation and maintenance of incident response teams, and the relevant plans, policies, and procedures, to
  - Minimize the impact to the populace, and
  - Minimize the disruption of services
- The creation of a statewide cybersecurity communication, collaboration, and information sharing network,
- Improving the creation and development of a cybersecurity workforce
- Assist DPS in Cybercrime investigations
- Creation of a state-wide strategic plan

THE OCDC

Strategic Objectives

- To build accessible and fundamental cybersecurity programs
- To take advantage of economies of scale
- To grow and strengthen the cybersecurity communications and relationships
- To create a resource base of policies, procedures, and assessment tools for use by all interested entities that work with the OCDC.
- To work with NSHE (Nevada System of Higher Education) entities to create a Cybersecurity workforce development
- To recruit staffing to support the legislative duties and functions assigned to the OCDC.

THE OCDC

- Current Staff
  - Aakin Patel - Administrator
  - Dianne Haigney – Cyber Threat Intelligence Analyst
  - Everett Wilson – Open Source Engineer

WHY THIS MATTERS

- SLTT Threats actively seen within the state
  - Example 1: Harry Reid Airport - BEC
  - Example 2: Nye County - BEC
  - Example 3: City of Reno - Cybersquatting
  - Example 4: Clark County UMC - Ransomware
  - Example 5: Truckee Meadows Water Authority - BEC
  - Example 6: Attack on state HR systems (NEATS) – State Actor?

WHY THIS MATTERS

- Non-SLTT Threats experienced:
  - Example 1: MGM Casinos - Ransomware
  - Example 2: IoT/OT Threats

CURRENT INITIATIVES

- Communications and Information Sharing
  - Already in place:
    - Newsletters
    - Communications channels and backchannels
      - Participation by and partnership with 53 SLTT entities
  - Planned:
    - State-wide threat sharing platform – Coordination with UNLV for student experience and workforce development
    - Statewide SOC

CURRENT INITIATIVES

- Support Services
  - Already in place:
    - Partnerships for incident response
    - Partnerships for assessments
  - Planned:
    - Software and Cybersecurity tools deployment
    - More formalized assessment process
    - Incident response exercise planning and testing
    - Internships / Labor assessment
    - Policy Libraries

CURRENT INITIATIVES

- Planned Programs
  - SLGCP Grant Program for support and assistance
    - Statewide SEIM/SOC
    - Incident Response Team
    - Training programs

CURRENT CHALLENGES

- Funding for these programs…
  - SLGCP Grant (Limited timespan)
  - State Budget
    - Severely restricted at this time
- Staffing
  - We do not have the staffing to support our legislative duties

POTENTIAL LEGISLATIVE THOUGHTS AND CONCERNS

- Reporting Requirements for Incidents
  - Public Organizations
  - Utilities and Infrastructure Groups
  - Private organizations with impactful scope
- Updated Cybercrime Laws
  - Cyberstalking/online harassment
  - Bitcoin ATMs
- Regulatory Update on scope of investigations re:personal devices

THANK YOU!

ANY QUESTIONS?