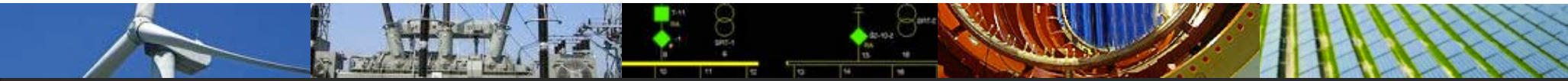
EnergySec
SECURING CRITICAL INFRASTRUCTURE

APPA Weekly Situation Report

Presented to:
American Public Power Association's (APPA)
Western Regional Cyber Security Summit
August 22, 2019

Weekly Situation Report In Brief

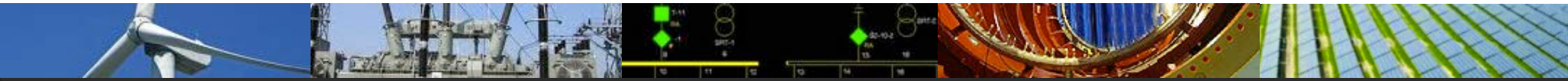
- Developed as part of a larger information sharing pilot project
- Developed by EnergySec under contract with APPA
- Currently 100% funded by DOE cooperative agreement
- Designed to provide a succinct summary of current security events and actionable items



EnergySec's Role

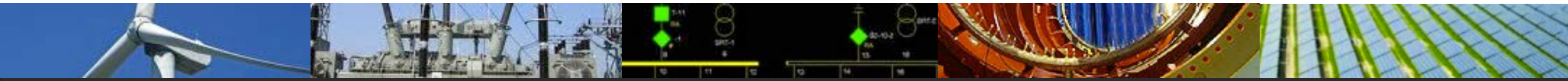
Provide cybersecurity analyst services to review, analyze, distill, and report on relevant cybersecurity threat feeds with the intent of providing actionable and usable information for APPA member organizations

Budgeted for roughly 1.5 FTEs for this project



About EnergySec

- Founded in 2003 as Energy Security Northwest (E-SecNW)
- Incorporated as non-profit (501c3) in 2008
- Selected by DOE for National Electric Sector Cybersecurity Organization (NESCO) grant in 2010
- Cybersecurity focused industry organization
- Existing contracts with DHS (cleared facility)
- Based in Portland, OR



Steve Parker

17 years cyber security in the electric sector

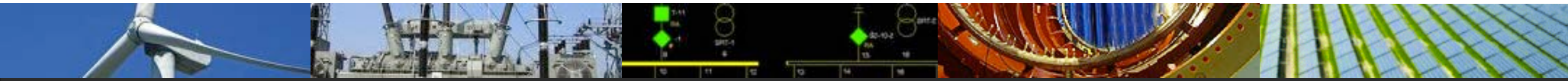
PacifiCorp 2001-2009

WECC (CIP Auditor) 2009-2010

EnergySec 2010- Present

Partner, Archer Security Group 2014 – Present

Certifications: CISA, CISSP



Andrew Zambrano

4 years cyber security in the electric sector

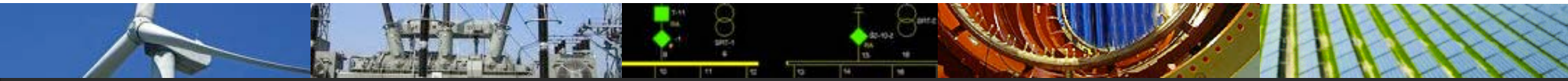
United States Marine Corps. 2001-2006

Navy Exchange Service Command (NEXCOM) 2009-2012

Transportation Security Administration 2013-2014

EnergySec 2015-Present

Degree: Cybersecurity/Networking



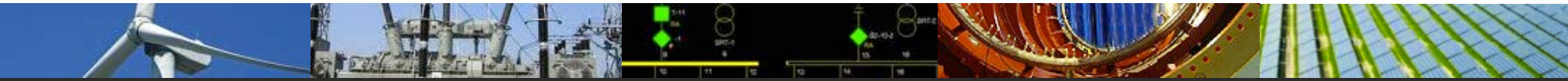
Sebastian Galvin

5 years cybersecurity/IT

IT Support, Recreation and Hospitality at Resort 2014 - 2016

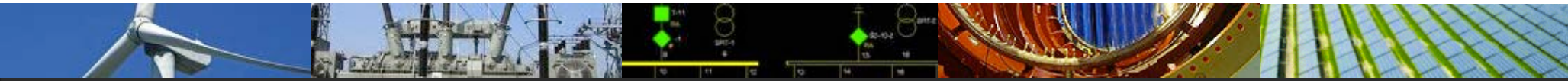
EnergySec 2016 – Present

Degree: Associates in Cybersecurity/Networking



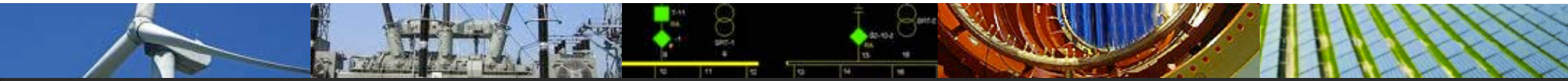
Ryan Bowers

- Mt. Hood Community College: Cyber Security and Networking Major. 2017-2019
- Norwich University: Information Warfare and Security Management Major. Current
- Heavy industrial maintenance technician, automation and controls background. (Aerospace, Amazon, Pharmaceuticals, food, etc..)
- Cyber Analyst for ICS with EnergySec



Current Status

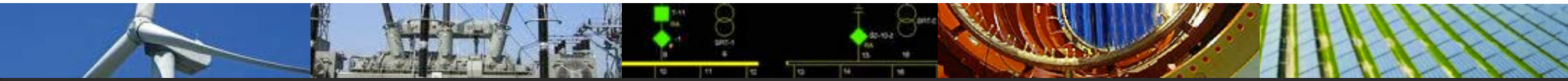
- Standard format developed and in use (Subject to change)
- WSRs being delivered weekly since May 16th
- Weekly coordination calls with APPA cybersecurity team
- Secure messaging (Armor Text) tool implemented and available



Distribution

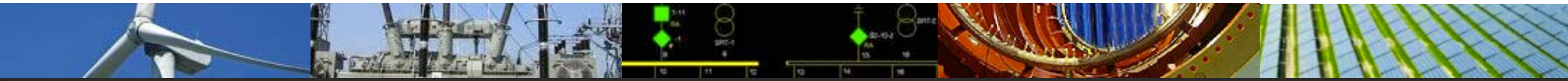
(Current) TLP/GREEN version being widely distributed via email

(Future) TLP/AMBER versions may be available via Armor Text



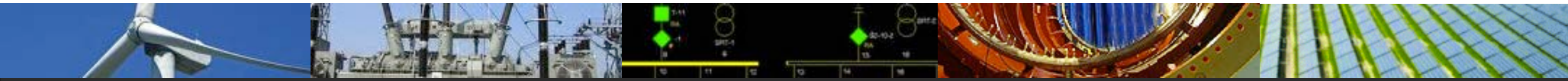
Information Sources (Current)

- Open Source Information
- APPA Sources
  - DOE/Government relationships
  - Membership
  - E-ISAC/MS-ISAC
  - Various other feeds
- EnergySec Sources
  - DHS CISCP Program
  - US-CERT/NCCIC
  - Non-public feeds via Anomali platform
  - Washington State Fusion Center



Information Sources (Future)

- Formal E-ISAC MOU (Nearly complete)
- MS-ISAC MOU (In progress)
- Direct Vendor feeds (Possible)
  - N-Dimension
  - Dragos
- Member submissions (highly desired)



Weekly Situation Report

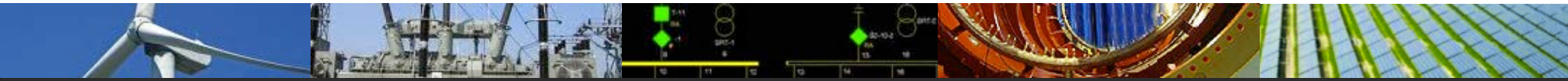
Weekly Situation Report

June 13, 2019

AMERICAN PUBLIC POWER ASSOCIATION

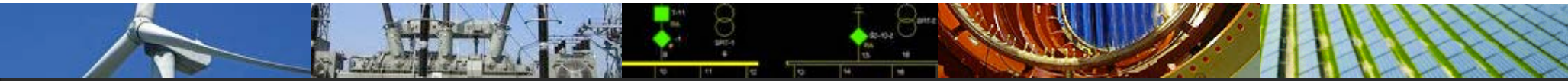
Summary

Section	Items	Source
Urgent Alerts/Vulnerabilities	- Critical Microsoft NTLM vulnerability - Vulnerability in Vim and NeoVim on Linux Distributions	CVE-2019-1040 CVE-2019-12735
Current Activity	- N/A	
Strategic Awareness	- Tool links Shodan data with Google Maps - HTTPS phishing	Github IC3
Information Request	- N/A	



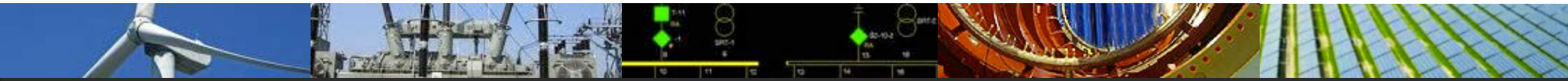
Alerts/Vulnerabilities

- This section will highlight and summarize key alerts or disclosed vulnerabilities that are likely to affect public power entities.
  - Control system specific with industry relevance
  - Significant general IT vulnerabilities
  - E-ISAC, US-CERT, and other relevant alerts



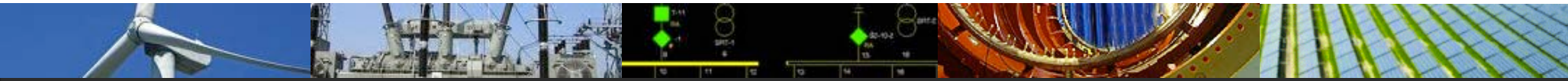
Alerts/Vulnerabilities

- Examples
  - Blue Keap
  - Urgent/11
  - NERC Alert on Supply Chain issues
- Feedback Needed
  - Relevance of specific issues
  - Extent to which certain technologies are deployed within public power



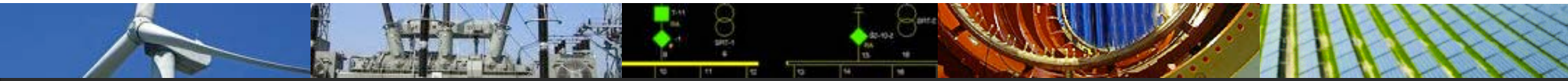
Current Activity

- This section will summarize current attack activity of significance to public power that was noted during the week
  - Actual Incidents
  - Campaigns
  - Significant phishing attempts



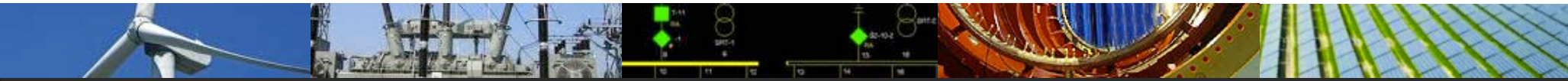
Current Activity

- Examples
  - Significant phishing activity
  - Ransomware
  - Microsoft Outlook Security Feature Bypass Vulnerability
- Feedback Needed
  - Relevance of issues
  - Reporting of activity (Significant reports via ISACs)



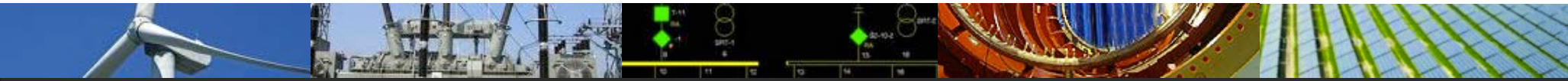
Strategic Awareness

- This section will discuss cybersecurity developments that do not require immediate action, but are relevant to longer term planning for cybersecurity defense
  - Emerging adversary capabilities and tactics
  - Industry trends
  - Threat scenarios
  - Adversary analysis



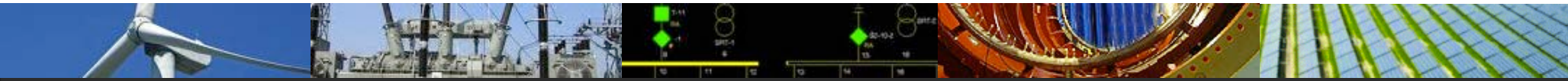
Strategic Awareness

- Examples
  - Geopolitical activity (US/Iran)
  - Increase in ransomware
  - Use of 3rd parties/MSP/MSSP in attacks
- Feedback needed
  - Input on relevance
  - Questions are welcome



Information Requests

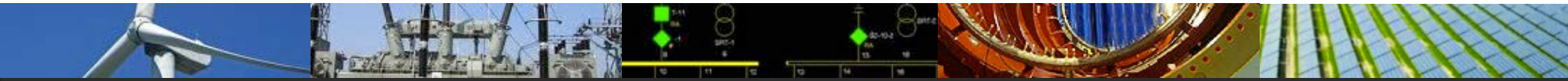
- From time to time we may request input on specific topics to provide a richer and more accurate context for our analysis
  - Requests are always optional, but any feedback will benefit the broader public power community
  - A discussion forum also exists on ArmorText for more real-time conversations



Questions

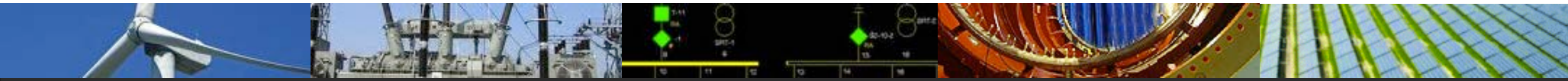
EnergySec's Role

- be available for regular phone calls with APPA staff and pilot group participants, as needed, to explain, review, or expand on information products developed under this statement of work

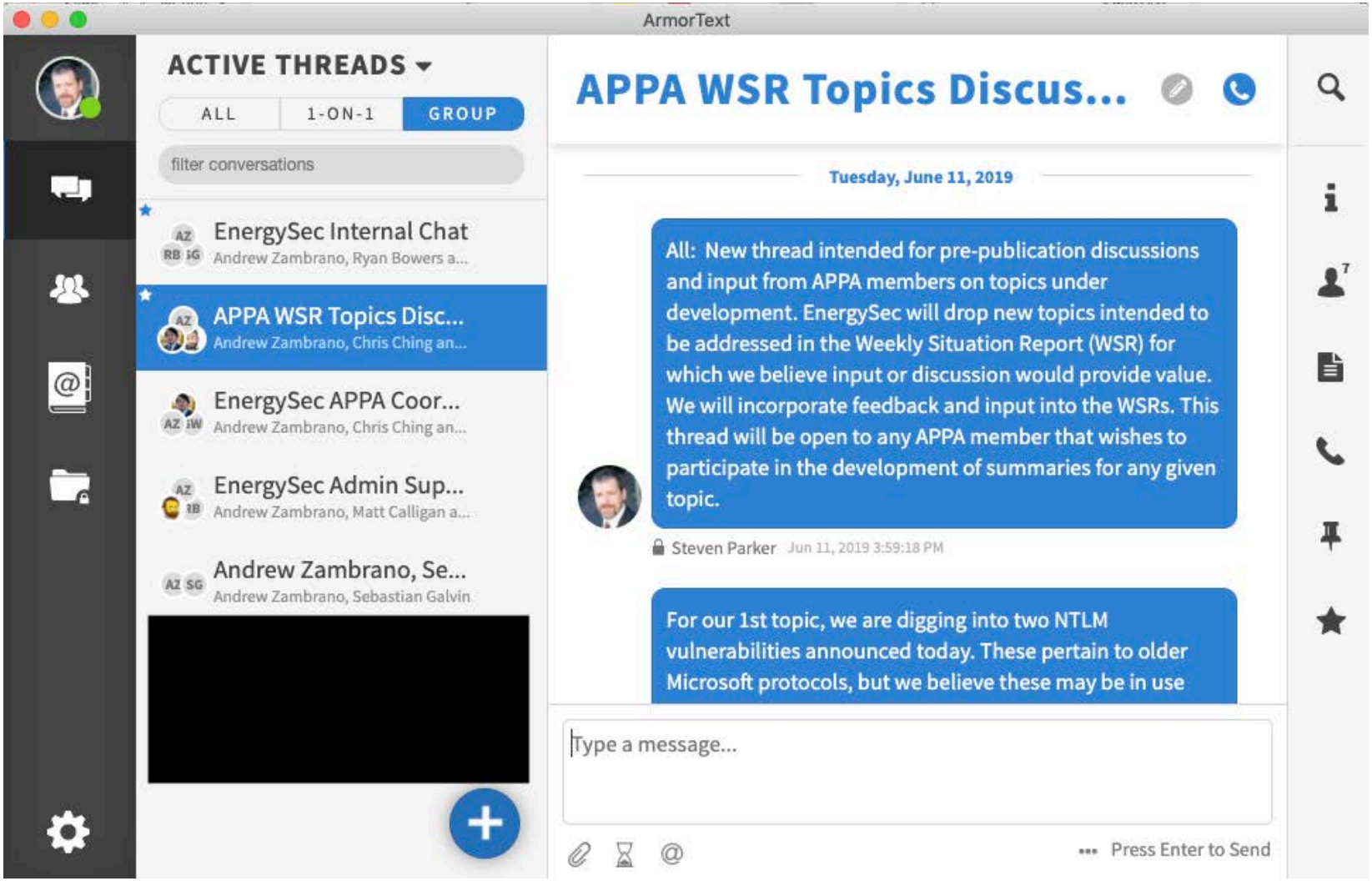


EnergySec's Role

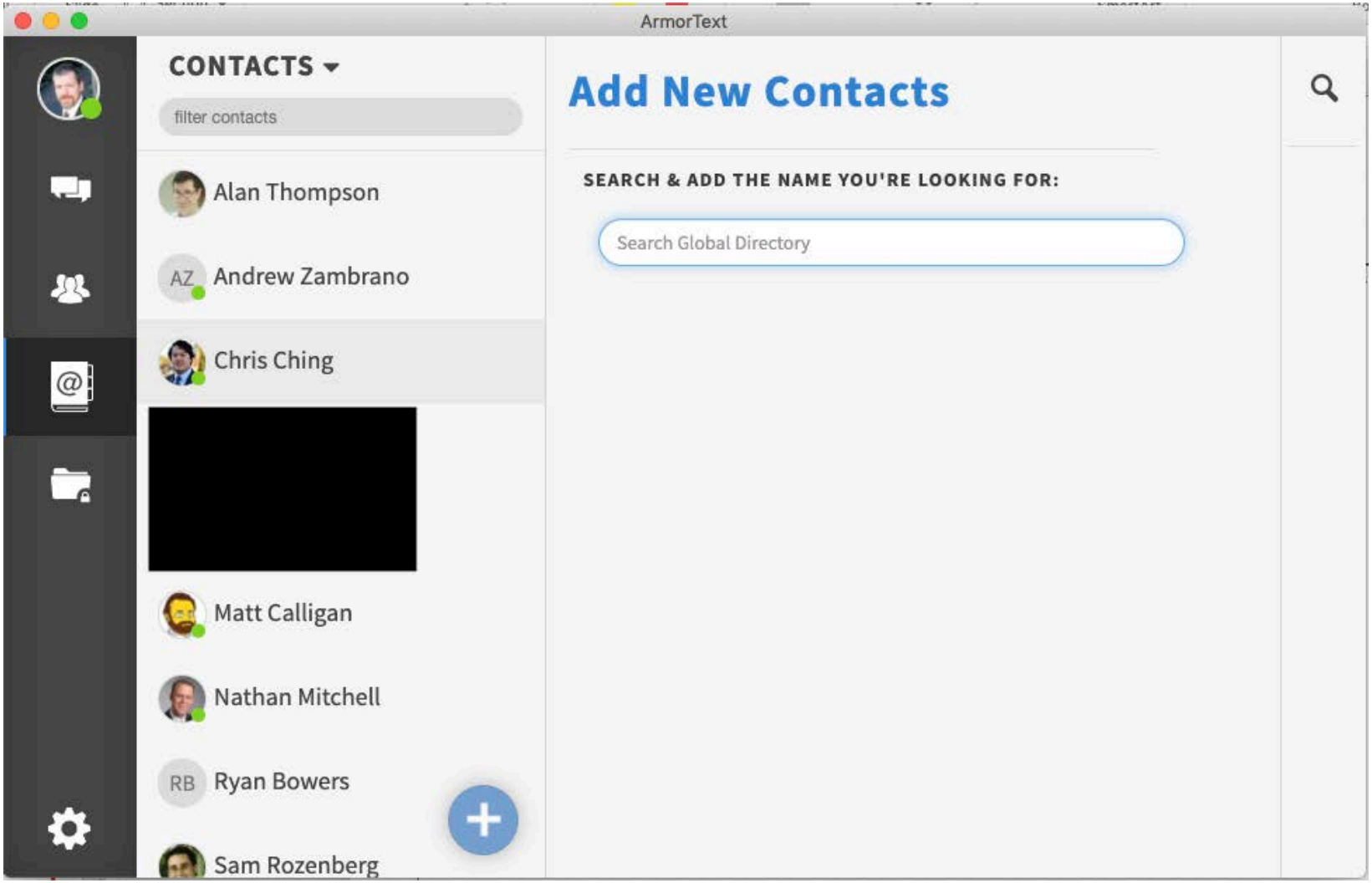
- EnergySec will develop practices for the use of relevant technology to develop, enhance, or deliver the products developed under this engagement



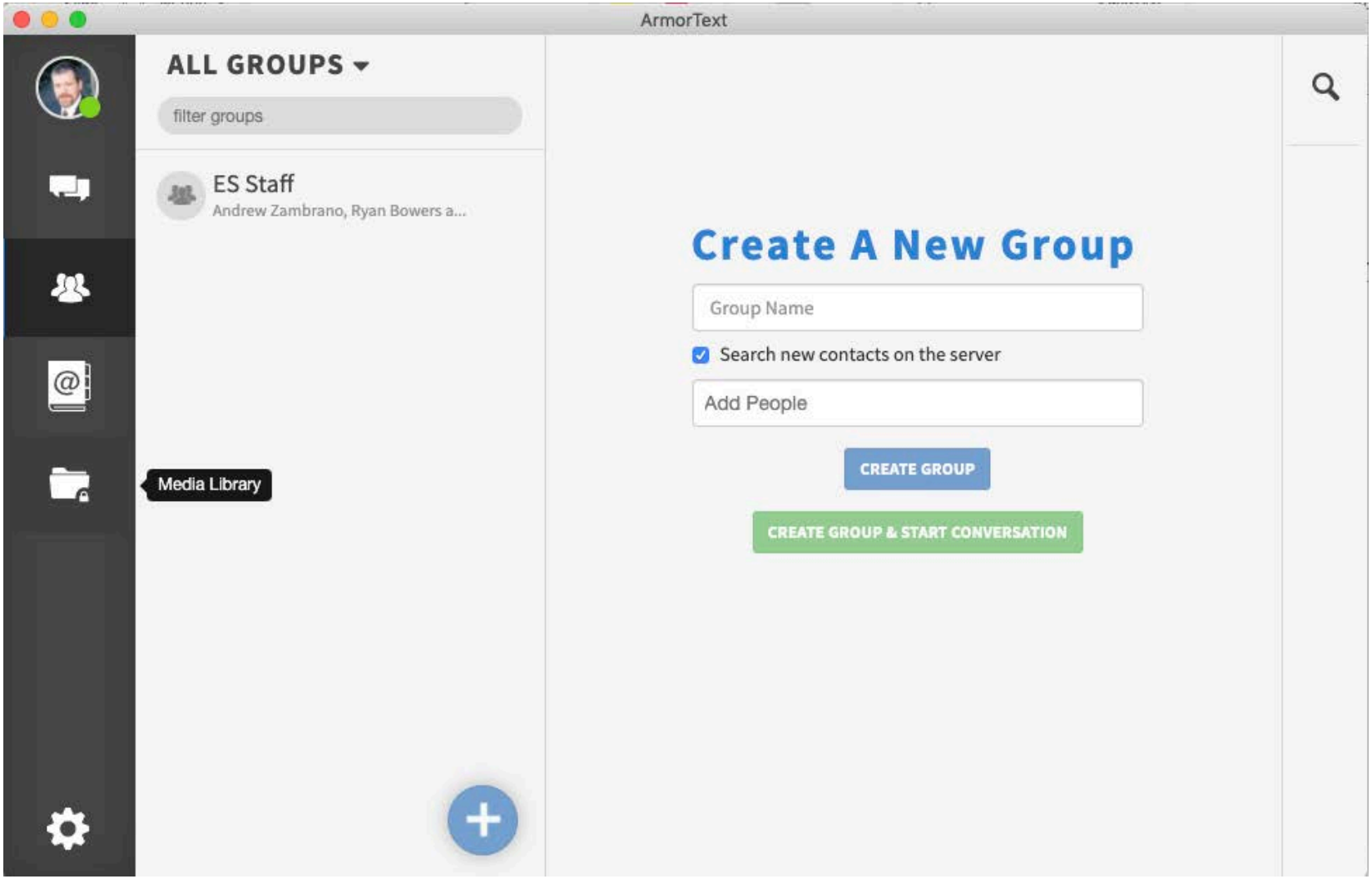
ArmorText


ArmorText
ACTIVE THREADS
ALL
1-ON-1
GROUP
filter conversations
EnergySec Internal Chat
Andrew Zambrano, Ryan Bowers a...
APPA WSR Topics Disc...
Andrew Zambrano, Chris Ching an...
EnergySec APPA Coor...
Andrew Zambrano, Chris Ching an...
EnergySec Admin Sup...
Andrew Zambrano, Matt Calligan a...
Andrew Zambrano, Se...
Andrew Zambrano, Sebastian Galvin
APPA WSR Topics Discus...
Tuesday, June 11, 2019
All: New thread intended for pre-publication discussions and input from APPA members on topics under development. EnergySec will drop new topics intended to be addressed in the Weekly Situation Report (WSR) for which we believe input or discussion would provide value. We will incorporate feedback and input into the WSRs. This thread will be open to any APPA member that wishes to participate in the development of summaries for any given topic.
Steven Parker Jun 11, 2019 3:59:18 PM
For our 1st topic, we are digging into two NTLM vulnerabilities announced today. These pertain to older Microsoft protocols, but we believe these may be in use
Type a message...
Press Enter to Send

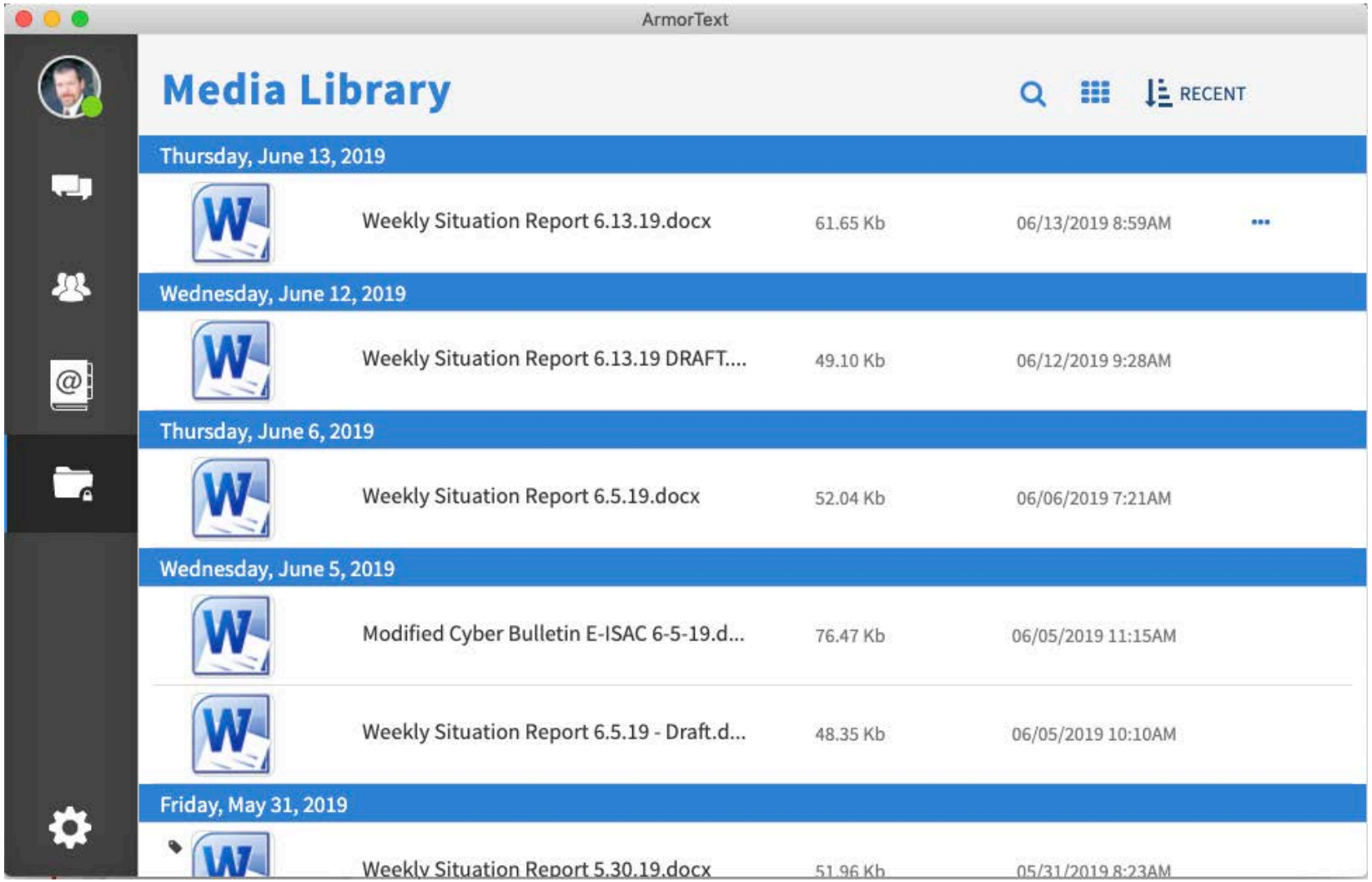
ArmorText


ArmorText
CONTACTS
filter contacts
Alan Thompson
AZ
Andrew Zambrano
Chris Ching
Matt Calligan
Nathan Mitchell
RB
Ryan Bowers
Sam Rozenberg
Add New Contacts
SEARCH & ADD THE NAME YOU'RE LOOKING FOR:
Search Global Directory

ArmorText


ArmorText
ALL GROUPS
filter groups
ES Staff
Andrew Zambrano, Ryan Bowers a...
Media Library
Create A New Group
Group Name
Search new contacts on the server
Add People
CREATE GROUP
CREATE GROUP & START CONVERSATION

ArmorText


ArmorText
Media Library
RECENT
Thursday, June 13, 2019
Weekly Situation Report 6.13.19.docx
61.65 Kb
06/13/2019 8:59AM
Wednesday, June 12, 2019
Weekly Situation Report 6.13.19 DRAFT....
49.10 Kb
06/12/2019 9:28AM
Thursday, June 6, 2019
Weekly Situation Report 6.5.19.docx
52.04 Kb
06/06/2019 7:21AM
Wednesday, June 5, 2019
Modified Cyber Bulletin E-ISAC 6-5-19.d...
76.47 Kb
06/05/2019 11:15AM
Weekly Situation Report 6.5.19 - Draft.d...
48.35 Kb
06/05/2019 10:10AM
Friday, May 31, 2019
Weekly Situation Report 5.30.19.docx
51.96 Kb
05/31/2019 8:23AM

Thank You

EnergySec
SECURING CRITICAL INFRASTRUCTURE

Steven H Parker
President, EnergySec
steve@energysec.org
503.905.2923 (desk)

Andrew Zambrano
Cybersecurity Analyst
andrew.zambrano@energysec.org
503.905.2925 (desk)

Sebastian Galvin
Cybersecurity Analyst
sebastian.galvin@energysec.org
503.905.2925 (desk)

Ryan Bowers
Cybersecurity Analyst
ryan.bowers@energysec.org
503.905.2921 (desk)