Contract No:

This document was prepared in conjunction with work accomplished under Contract No. 89303321CEM000080 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

This work was prepared under an agreement with and funded by the U.S. Government. Neither the U.S. Government or its employees, nor any of its contractors, subcontractors or their employees, makes any express or implied:

1) warranty or assumes any legal liability for the accuracy, completeness, or for the use or results of such use of any information, product, or process disclosed; or

2) representation that such use or results of such use would not infringe privately owned rights; or

3) endorsement or recommendation of any specifically identified commercial product, process, or service.

Any views and opinions of authors expressed in this work do not necessarily state or reflect those of the United States Government, or its contractors, or subcontractors.

Savannah River
National Laboratory®

A U.S. DEPARTMENT OF ENERGY NATIONAL LAB • SAVANNAH RIVER SITE • AIKEN, SC • USA

Power Over Ethernet Investigation Report

Dillon Tauscher

October 19, 2021

B-RPT-A-00001, Revision 0

SRNL.DOE.GOV

DISCLAIMER

This work was prepared under an agreement with and funded by the U.S. Government. Neither the U.S. Government or its employees, nor any of its contractors, subcontractors or their employees, makes any express or implied:

1. warranty or assumes any legal liability for the accuracy, completeness, or for the use or results of such use of any information, product, or process disclosed; or
2. representation that such use or results of such use would not infringe privately owned rights; or
3. endorsement or recommendation of any specifically identified commercial product, process, or service.

Any views and opinions of authors expressed in this work do not necessarily state or reflect those of the United States Government, or its contractors, or subcontractors.

Printed in the United States of America

Prepared for
U.S. Department of Energy

B-RPT-A-00001
Revision 0

Keywords: *Power Over Ethernet, POE, University Collaboration, Augusta University, Georgia Cyber Center, GCC,*

Retention: *Varies*

Power Over Ethernet Investigation Report

Dillon Tauscher

October 4, 2021

Savannah River National Laboratory is operated by Battelle Savannah River Alliance for the U.S. Department of Energy under Contract No. 89303321CEM000080.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC/DC	Alternating Current and Direct Current
ARP	Address Resolution Protocol
AU	Augusta University
G-CIIC	Georgia Cyber Center-Critical Infrastructure, Industrial Control System Cybersecurity
GCC	Georgia Cyber Center
IP	Internet Protocol
NBNS	NetBIOS Name Service
PoE	Power over Ethernet
SRNL	Savannah River National Laboratory
WAP	Wireless Access Point

1.0 Introduction

This report provides insight into collaboration between Savannah River National Laboratory's (SRNL) Global Security Directorate, Augusta University (AU) and the Georgia Cyber Center (GCC) team with regards to device analysis, investigation, and R&D efforts. Most recently, the GCC/AU team approached SRNL to receive cybersecurity expertise in a joint effort to identify differences between a potentially questionable PoE injector recovered by Columbia County and an identical one purchased by the GCC. The questionable device was installed at a fire station operated in Columbia County, shown in the figure 1-1 below.

While there were no notable anomalies believed to be present with malicious intent, SRNL utilized various capabilities (X-RAY, Network Traffic Analysis, Internal Component Analysis, Counterintelligence) to demonstrate technical prowess covering a multitude of cybersecurity domains. SRNL leveraged presence at the Georgia Cyber Center-Critical Infrastructure, Industrial Control System (ICS), and Cybersecurity (G-CIIC) lab hosted at the GCC to perform detailed and isolated device capability testing while being in proximity of collaboration partners. Through this joint effort with AU and the GCC innovation team, SRNL not only demonstrated the capability to discover circuitry level discrepancies, but developed a streamlined process for receipt, analysis and reporting of physical evidence in future local and national-level cybersecurity investigations. Furthermore, the GCC team and Augusta University enhanced working relationships with local communities regarding information and device security, processes for potential graduate research opportunities, and joint-investigative procedures with SRNL. A list of cybersecurity network recommendations was presented as a result of this investigation.

Figure 1-1. Fire Station in Columbia County

2.0 Accomplishments

During this investigation, SRNL accomplished multiple monumental objectives-- establishing a baseline for future cybersecurity endeavors.

1. Developed and executed a joint process for investigating hardware, including a mock-up of custody/transfer logs.
2. Assisted the local county by providing feedback as to whether the device is malicious or recommend further investigation into connected hardware.
3. Established a collaborative technical relationship with GCC and AU employees, utilizing SRNL (S-CIIC, G-CIIC, etc.) and University capabilities.
4. Enhanced SRNL's reputation in the cybersecurity community.

3.0 Incident Background

On Thursday April 15, 2021, Glenn Kennedy, the Deputy County Manager for Columbia County, Georgia, contacted the GCC about a potential breach of the Columbia County IT network at an unspecified fire department location. A PoE injector was found on their network, connected to a Cisco 2901 Integrated Service Router. The device was placed by an individual who posed to be working for County Information Technology Services. Columbia County surrendered it to the GCC for further investigation due to lack of evidence and did not want the device returned. The GCC immediately purchased the same device model for comparison and later engaged SRNL to leverage technical capabilities and cybersecurity expertise for non-destructive and potentially destructive analysis.

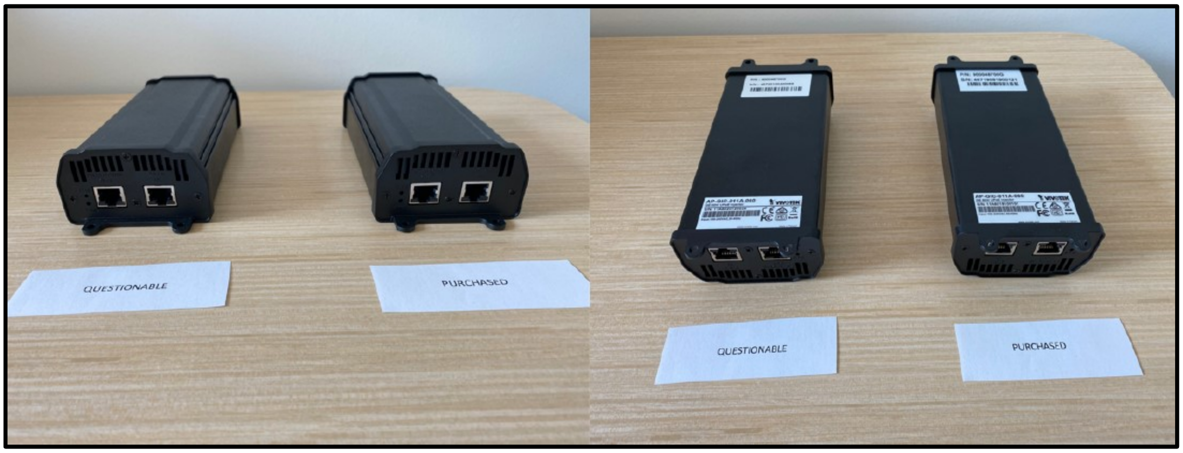


Figure 3-1. Purchased and Questionable Power Over Ethernet Devices

4.0 Investigative Process

4.1 X-RAY

On Thursday August 5, 2021, the questionable and purchased devices were transferred to SRNL personnel for X-RAY and visual inspection of both devices to determine if there was any physical tampering. Upon further investigation, SRNL discovered that there were minute differences in soldering between the devices. A diagram depicting the differences is shown below. SRNL and the GCC team reconvened to discuss findings and review X-RAY imagery in unison to ensure that there were no overlooked anomalies.

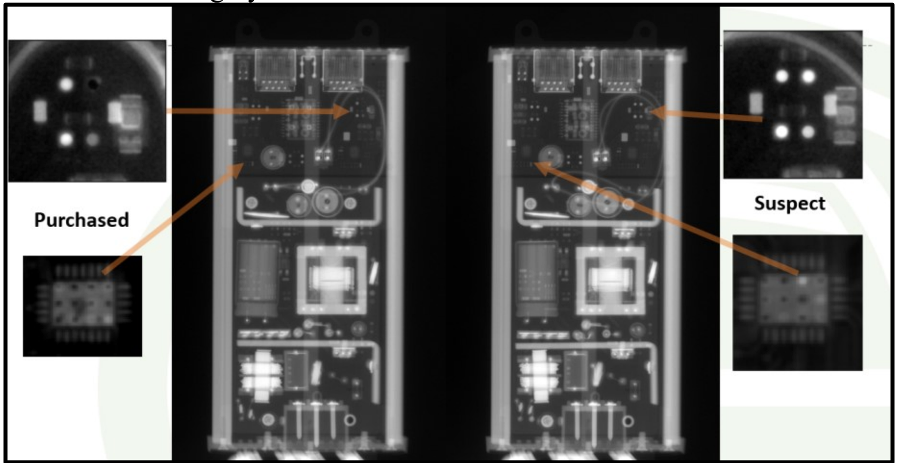


Figure 4-1. Radiograph Comparison

4.2 **Fire Station Visit**

After the X-RAY imagery analysis was completed, the team met with the fire station in question to gain insight into network topology and physical security practices at the location. The current PoE device can be seen on the bottom right of the wooden board, while the suspect device was installed on the bottom left.

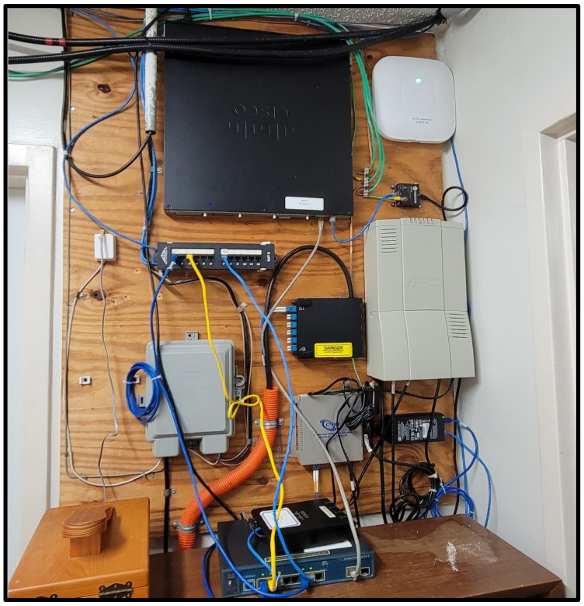


Figure 4-2. Fire Station Network

The fire station has already implemented physical access policies for visitors, having the current shift contact the information technology lead before allowing any work to take place on IT systems. The fire station performed security log analysis on their network and found no suspicious activity. Following cybersecurity best practices, they reset the Cisco integrated router/switch to default configuration. The IT lead for the fire station provided additional equipment for the team to analyze (one Cisco AIR-CAP2602I-A-K9 Wireless Access Point).

4.3 **Network Traffic Analysis**

Two SRNL Engineers from the Global Security Directorate met at the G-CIIC to perform a generic network analysis of the purchased and questionable devices and their connectivity to the wireless access point with an isolated system.

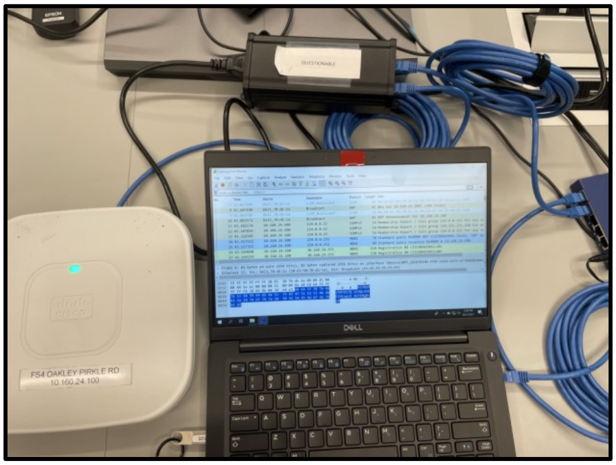
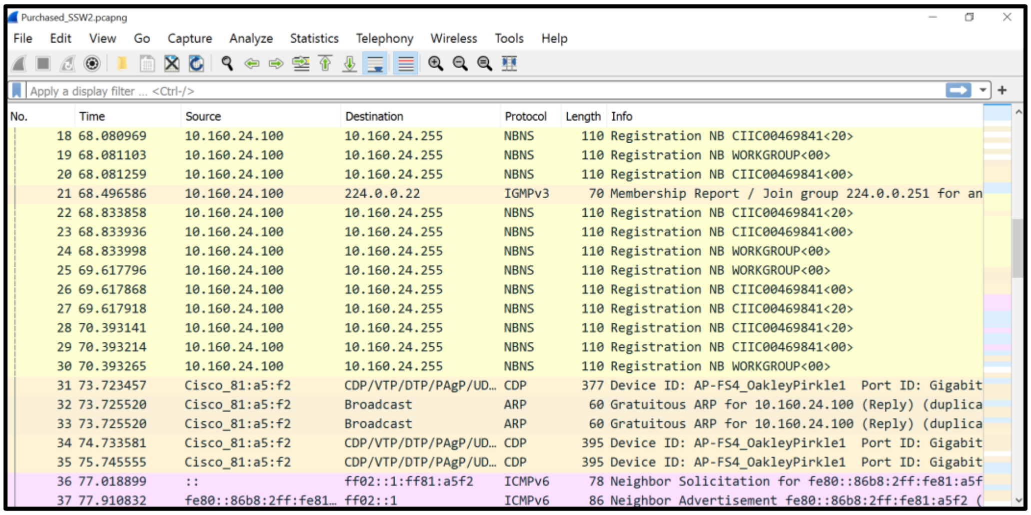


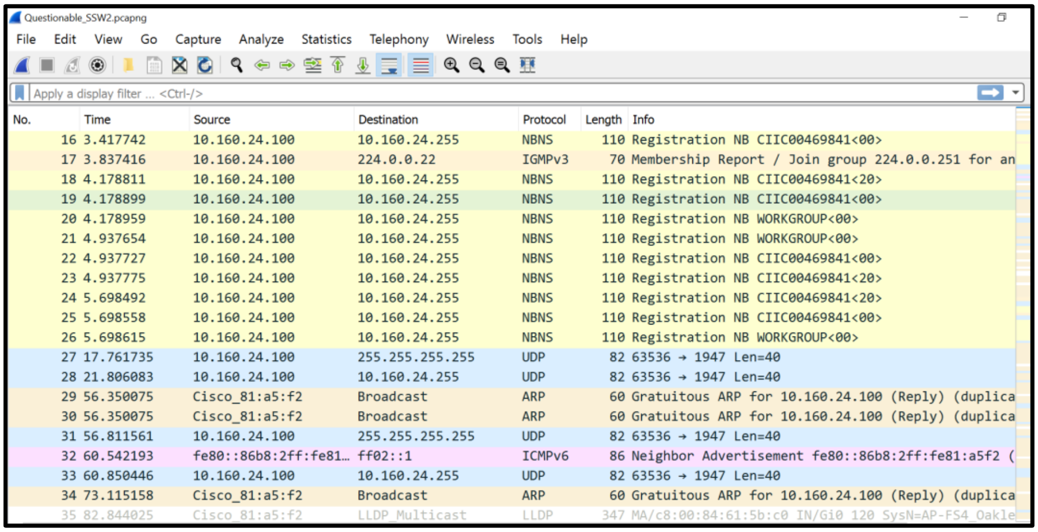
Figure 4-3. Network Traffic Analysis

Upon further investigation using Wireshark and Kali Linux, there were no notably suspicious pieces of traffic originating from any of the analyzed devices. The traffic consisted of standard gratuitous ARP (router solicitation via address resolution protocol), NetBIOS Name Service (NBNS), and membership reports for connected devices via hostnames and IP addresses. Additional Wireshark packet captures of the individual PoE devices connected to the provided Wireless Access Point (WAP) and an isolated machine can be seen below.



No.	Time	Source	Destination	Protocol	Length	Info
18	68.080969	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
19	68.081103	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
20	68.081259	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
21	68.496586	10.160.24.100	224.0.0.22	IGMPv3	70	Membership Report / Join group 224.0.0.251 for an
22	68.833858	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
23	68.833936	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
24	68.833998	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
25	69.617796	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
26	69.617868	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
27	69.617918	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
28	70.393141	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
29	70.393214	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
30	70.393265	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
31	73.723457	Cisco_81:a5:f2	CDP/VTP/DTP/PAgP/UD…	CDP	377	Device ID: AP-FS4_OakleyPirkle1 Port ID: Gigabit
32	73.725520	Cisco_81:a5:f2	Broadcast	ARP	60	Gratuitous ARP for 10.160.24.100 (Reply) (duplica
33	73.725520	Cisco_81:a5:f2	Broadcast	ARP	60	Gratuitous ARP for 10.160.24.100 (Reply) (duplica
34	74.733581	Cisco_81:a5:f2	CDP/VTP/DTP/PAgP/UD…	CDP	395	Device ID: AP-FS4_OakleyPirkle1 Port ID: Gigabit
35	75.745555	Cisco_81:a5:f2	CDP/VTP/DTP/PAgP/UD…	CDP	395	Device ID: AP-FS4_OakleyPirkle1 Port ID: Gigabit
36	77.018899	::	ff02::1:ff81:a5f2	ICMPv6	78	Neighbor Solicitation for fe80::86b8:2ff:fe81:a5f
37	77.910832	fe80::86b8:2ff:fe81…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::86b8:2ff:fe81:a5f2 (

Figure 4-4. Purchased PoE Device Traffic



No.	Time	Source	Destination	Protocol	Length	Info
16	3.417742	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
17	3.837416	10.160.24.100	224.0.0.22	IGMPv3	70	Membership Report / Join group 224.0.0.251 for an
18	4.178811	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
19	4.178899	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
20	4.178959	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
21	4.937654	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
22	4.937727	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
23	4.937775	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
24	5.698492	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<20>
25	5.698558	10.160.24.100	10.160.24.255	NBNS	110	Registration NB CIIC00469841<00>
26	5.698615	10.160.24.100	10.160.24.255	NBNS	110	Registration NB WORKGROUP<00>
27	17.761735	10.160.24.100	255.255.255.255	UDP	82	63536 → 1947 Len=40
28	21.806083	10.160.24.100	10.160.24.255	UDP	82	63536 → 1947 Len=40
29	56.350075	Cisco_81:a5:f2	Broadcast	ARP	60	Gratuitous ARP for 10.160.24.100 (Reply) (duplica
30	56.350075	Cisco_81:a5:f2	Broadcast	ARP	60	Gratuitous ARP for 10.160.24.100 (Reply) (duplica
31	56.811561	10.160.24.100	255.255.255.255	UDP	82	63536 → 1947 Len=40
32	60.542193	fe80::86b8:2ff:fe81…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::86b8:2ff:fe81:a5f2 (
33	60.850446	10.160.24.100	10.160.24.255	UDP	82	63536 → 1947 Len=40
34	73.115158	Cisco_81:a5:f2	Broadcast	ARP	60	Gratuitous ARP for 10.160.24.100 (Reply) (duplica
35	82.844025	Cisco_81:a5:f2	LLDP_Multicast	LLDP	347	MA/c8:00:84:61:5b:c0 IN/Gi0 120 SysN=AP-FS4_Oakle

Figure 4-5. Questionable PoE Device Traffic

4.4 Internal Hardware Analysis

After the network capability testing was conducted, the team brought the devices back to SRNL for isolated analysis via de-constructive methods. No circuitry was found on the AC/DC board that would indicate the presence of a PLComms modem, and the only chip present was a standard switching controller. When compared, the PoE boards on the purchased and questionable devices shared similar circuitry construction other than slight indications of separate manufacture runs indicated by different laser etching between boards (purchased board has microchip in 2018 with date code of 39th week of

2017, questionable board has no Microsemi logo and date code of 39th week 2019). Based on standard visual inspection, the devices are similar, and nothing appears out of the ordinary. A visual inspection of the PoE interior hardware can be seen in the figure below.

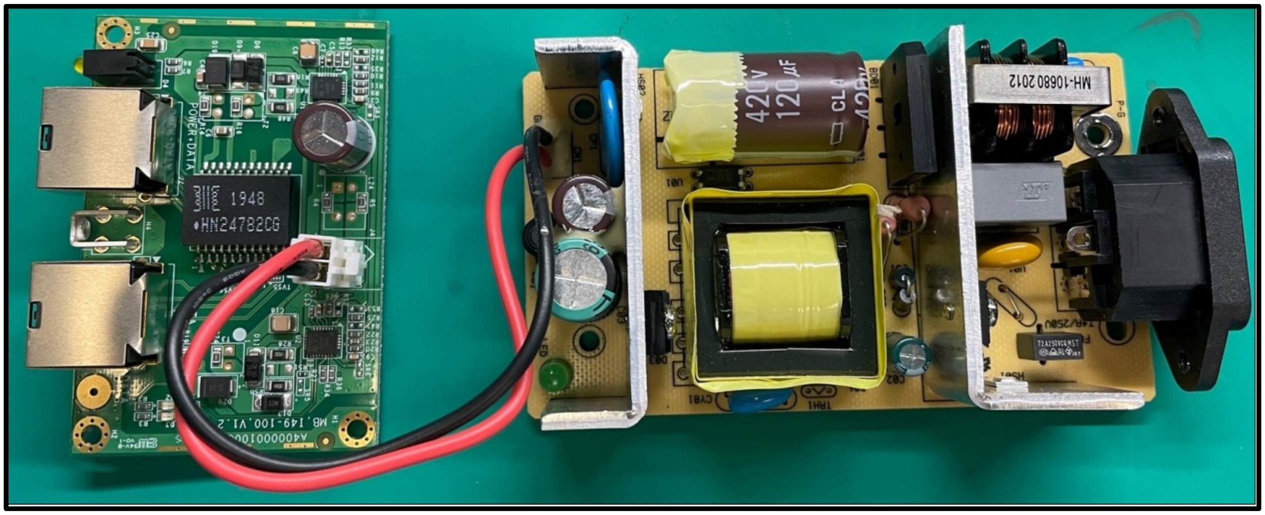


Figure 4-6. PoE Device Interior

5.0 Recommendations and Lessons Learned

The team suggests that the fire station review their server settings and ensure that NBNS is disabled, unless necessary- to prevent the potential of NBNS spoofing attacks, web traffic sniffing, and potential hashed credential grabs. Generally, corporate networks can keep up with users based on the domain name system (DNS) alone. Ports can also be closed on the router to prevent requests from occurring, or the local firewall can be modified to only accept trusted connections based on access lists, router history, or credentialed methods.

The SRNL Cybersecurity and Threat Assessments group developed a strong working relationship with several other groups at SRNL and will consult them for expertise in counterintelligence (vendor research and device origin), evidence handling, and X-RAY imagery, allowing SRNL to provide a unique capability within the local and national cybersecurity communities for critical R&D and incident response.

6.0 Contributors

Augusta University- Dr. Michael Nowatkowski
Georgia Cyber Center- Dr. Clay Moody
Savannah River National Laboratory-
Dillon Tauscher, Harrison Howell, David Immel, Nicholas Deroller, Steven Dameron, Richard Poland