ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Cybersecurity Potential of the Savannah River Site

Phase 1 Report

June 2018

Center for SPACE WARFARE STUDIES

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Center for Cyber-Influence Operations Studies CCIOS

Support ICIT

Through objective research, publications and educational initiatives, the Institute for Critical Infrastructure Technology, a 501(c)(3) cybersecurity think tank located in Washington, D.C., is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cybercriminals, nation-states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policymakers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Contents

Abstract

According to annual DOE OIG evaluations, cybersecurity and cyber-hygiene within Energy sector entities under the DOE are lacking. Sensitive information, vital systems, and critical assets are exposed to malicious compromise as a result. In response to the apparent need, ICIT conducted a strategic assessment to better understand the cybersecurity posture of the DOE and DHS, proposed cybersecurity policies and strategies, and whether the Savannah River Site (SRS) resources, facilities, and capabilities could be leveraged to enhance the security and resiliency of the critical infrastructure assets. Based on interviews and the overwhelmingly positive findings of Phase I research, ICIT concludes that there is a strong case for the SRS to be developed as a cybersecurity leader capable of fulfilling the needs and missions of national security and multiple critical infrastructure sectors.

The SRS Community Reuse Organization (SRSCRO) brought this concept to the attention of ICIT in the first quarter of 2018. The SRSCRO is a 501(c)(3) private nonprofit organization charged with developing and implementing a comprehensive strategy to diversify the economy of a five-county region in the Central Savannah River Area of Georgia and South Carolina. SRSCRO counties include Aiken, Allendale, and Barnwell in South Carolina and Richmond and Columbia in Georgia.

Introduction

The Savannah River Site covers 310 square miles near Aiken, South Carolina. The Site is situated in parts of Aiken, Barnwell, and Allendale counties in South Carolina. However, the impact area of the Site extends into Georgia to Richmond and Columbia counties. This five-county area is the SRS Impact Area. The Savannah River Site has been a key economic driver in the surrounding five-county region since its establishment in the early 1950s.

SRS was constructed during the early 1950s to produce the basic materials used in the fabrication of nuclear weapons, primarily tritium and plutonium-239. Five reactors were built to produce these materials. Several support facilities were also built including two chemical separations plants, a heavy water extraction plant, a nuclear fuel and target fabrication facility, a tritium extraction facility, and waste management facilities. Between 1953 and 1988, SRS produced and shipped about 36 metric tons of plutonium.

After 50 years of producing nuclear materials for defense and non-defense uses, SRS shifted its strategic direction and resources from nuclear weapons materials production to the cleanup of the nuclear waste and environmental contamination created during production. In support of national defense and US nonproliferation efforts, SRS now processes and stores nuclear materials.

The primary Department of Energy programs and mission areas at SRS are Environmental Management (EM) and National Nuclear Security Administration (NNSA). EM represents 68 percent of the current budget. This includes management, stabilization, and disposition of nuclear materials; management and disposition of solid, liquid and transuranic wastes; spent fuel management; and environmental remediation and cleanup. Thirty-two percent of the budget is related to the NNSA including tritium operations and extraction; helium-3 recovery; nonproliferation support; mixed oxide (MOX) fuel fabrication; uranium blending and shipping; and foreign fuel receipts.

SRS is also home to the Savannah River National Laboratory (SRNL). It is the newest of all the National Laboratories and the only laboratory under DOE's Environmental Management purview. SRNL is a small multi-program, multi-purpose laboratory compared to other National Laboratories. However, it is uniquely positioned to meet current and future energy and national security challenges and missions.

Applied research is one unique aspect offered by SRNL. As an applied research and development laboratory, SRNL supports customers at SRS, throughout DOE, at other federal agencies, across the country, and around the world. The laboratory currently serves the nation in three major program areas: (1) National and Homeland Security, (2) Energy Security, and (3) Environmental and Chemical Process Technology. For example, SRNL is the FBI "Hub Lab" for pre-detonation forensics.

The "global" Savannah River Site is uniquely and ideally positioned to assist in the cybersecurity of America's critical infrastructure from within the Greater Augusta/Aiken MSA Region by leveraging its local synergies and partnerships; employing its physical, digital, and human assets; and capitalizing on the stable economy and growing workforce of the region.

Every day, critical infrastructure assets are targeted by hyper-evolving nation-state threat actors, digital mercenary, and cybercriminals. Systemically lackadaisical cyber-hygiene, archaic legacy systems, and intrinsic software vulnerabilities ensure that targeted assets are compromised and that adversaries continue to exfiltrate sensitive PII, PHI, and IP; damage vital systems; and laterally infect associated targets. The development of innovative and holistic Information Security strategies, products, and services necessitates collaboration between federal, state, and local government, critical infrastructure organizations, academia, and regional industry partners. The Savannah River Site is one of only a few organizations in the nation capable of meaningful stakeholder-driven collaboration and research that could reshape American cybersecurity.

The security and resiliency of the U.S. Energy Sector, often considered to be *the* point-of-failure for all other critical infrastructure sectors, is of paramount importance to the Nation's economy, public health and safety, and way of life. The U.S. Department of Energy's (DoE) classified and non-classified portfolio of responsibilities touches virtually every aspect of our energy sector, including energy manufacturers and suppliers, the energy grid, and our Nation's nuclear weapons stockpile. Existing resources, facilities, and capabilities found in the Savanah

River Site (SRS) region may provide the ideal solution to mitigate threats to the DOE and other critical infrastructure organizations.

The Augusta/Aiken MSA region is emerging as one of America's innovation hubs due to the ongoing evolution of its technology, defense, and cyber economies. In August 2017, the Alliance for Fort Gordon announced the launch of the partnership of military, business, and civic leadership known broadly as the "Fort Gordon Cyber District." The district includes Richmond, Columbia, Burke, McDuffie, and Lincoln counties in Georgia, and Aiken, Barnwell, Allendale, and Edgefield counties in South Carolina. Factors in the region position the Augusta area to be welcoming and attractive to cybersecurity talent and businesses. The alliance is helping to shape education, workforce development, innovation, entrepreneurship and marketing centered on the development of the local cyber community [1].

Cybersecurity – the protection of computer networks and programs, data, and other digital assets from attack or unauthorized access or alteration– is becoming a booming part of the Augusta area's economics. By 2020 the vast U.S. Army Cyber Command will transfer to Fort Gordon, the region's largest employer. Further, the $95 million Hull McKnight Georgia Cyber Innovation and Training Center, now under construction downtown on Reynolds Street, will be the centerpiece of Augusta University's Cyber Campus [2].

The vast cybersecurity and training centers located at Fort Gordon already make it one of the largest employers in the area; it has an estimated annual economic impact of $2.26 billion on the region. Additionally, more than $211 million in construction is ongoing at Fort Gordon, and project upgrades, renovations, and construction is expected to contribute over $1.4 billion to the region over the next decade [1].

The Greater Augusta/Aiken MSA Region is in the middle of an economic renaissance. Each of the major three counties – Aiken, Columbia, and Richmond Counties - are seeing a variety of new investment in the development of new products and services to support technology companies such as office building, the development of new education programs, the development new quality of life offerings to bolster the arts, and infrastructure investment to improve the daily commute. The region has demonstrated sustained and stable economic growth. Opportunities for new investment, talent recruitment and a workforce with transferable skills that understand the nature of government contracting, cybersecurity, and defense are believed to be one result of the growth. Fort Gordon is planning on investing nearly $2 billion over the next 7 to 10 years; however, overall more than $4 billion may be invested in the region in the near future. Additionally, private manufacturers and the Savannah River Site are expected to invest in the area as development evolves. Region population growth predictions based on economic projections anticipate an increase of more than 130,000 residents between 2015 and 2035, although innovation, such as adoption of cybersecurity leadership initiatives at the SRS, could galvanize more significant investment and growth.

Positives

- Strong regional synergies and collaborative initiatives.
- The SRS is ideally situated and equipped to play a role in critical infrastructure cybersecurity.
- Development costs in the region are low.
- Investment and growth in the area are historically stable and is likely to increase.
- Low cost of living and regional incentives may draw external talent to the area and SRS.

America Needs the Cybersecurity Leadership the SRS Can Provide

America's homes, business, and services depend on the resiliency of the Energy sector. The electric grid is so essential to everyday life that it is literally the only critical infrastructure network that is visible in every city, business, or home in the nation. Citizens depend so much on the electric grid and the energy production facilities that support it that their brains barely register the powerlines overhead or the substations in town. Electricity is like air in that many do not think about it unless it is not continuously available. Only during a power failure, when control over temperature management, entertainment, cooking, refrigeration, light, and services, are unavailable do citizens genuinely realize their dependency on the Energy sector. When citizens lose access to electricity, public resentment grows and crime increases. If the disruption persists, lives may be at risk.

The Energy Sector is a primary target of nation-state and mercenary APTs, hacktivists, cyber-jihadists and other threat actors because it is the backbone of the nation. Every other critical infrastructure sector depends on the continued confidentiality, availability, integrity, and resiliency of energy sector infrastructure. Over 70% of energy firms are concerned about high-profile ICS/SCADA attacks such as Triton/Trisis, Industroyer/CrashOverride, and other evolving malware. 95% of energy and oil & gas firms are concerned about operational outages, shutdowns, and physical injuries due to cyberattacks.

The United States Energy sector is dependent on an intricate amalgamation of interwoven networks of antiquated legacy systems and interconnected under-protected modern technology. A malware campaign cannot entirely take down the grid because it consists of a distributed and interwoven network of utility companies, transmission networks, distribution hubs, and other entities that are too complex for anyone attacker to singlehandedly dismantle. Additionally, redundancy systems and physical fail-safes protect the grid from catastrophe. Nevertheless, a dedicated adversary can impact targeted regions and inflict significant harm through disruption of energy delivery, cyber-kinetic attacks on vital systems, and the unauthorized access or alteration of critical data. Repairs to energy systems are expensive. Every minute electricity delivery is disrupted costs money and lives.

Example Threat Actors

Deep Panda/ APT 19/ Shell Crew/ Black Vine/ Kung Fu Kitten (Chinese APT)

Deep Panda is a state-sponsored threat responsible for some of the most prolific attacks against the Energy, Healthcare, and Aerospace since at least 2012.

Deep Panda has conducted multiple sizable campaigns against United States Federal government agencies and major western organizations. For example, in one facet of the Deep Panda campaign, it concurrently attacked the United States Office of Personnel Management, the Anthem healthcare network, United Airlines, and other entities. A vast majority, ~80%, of Deep Panda targets are American.

Deep Panda is the first Chinese state-sponsored group to target PII, though the group tends to focus on operational design data. The information is rarely if ever, exploited for financial gain. Instead, the data is used to create dossiers, to monitor populations and systems, or to leverage against individuals who concern the Chinese government.

Deep Panda is also believed to be responsible for the two 2015 OPM breaches. Further, Deep Panda breached United Airlines in 2015 and stole departure and destination records. The health, OPM, and travel records stolen by Deep Panda can be aggregated to catastrophically impact the United States government over time. The adversary or their parent nation-state can use the stolen information to build a database of US employees and contractors for espionage purposes. The data can also be used to identify United States agents in the country or to identify Chinese assets who assist United States intelligence efforts. Moreover, the information obtained in the OPM breach could be combined with the information stolen in Deep Panda's healthcare breaches or with information publically released in incidents, such as the Ashley Madison breach, to manipulate or leverage pressure against specific United States citizens to serve the Chinese agenda.

Deep Panda relies on the Sakurel Trojan, the Hurix Trojan, and the Mivast backdoor in its attacks. Deep Panda is believed to have developed all of the malware themselves. Characteristics in the malware code are shared between all three malware. Further, each malware is capable of opening a named pipe back door, tools to collect and exfiltrate system data, the ability to execute arbitrary code, and the ability to create, modify, and delete registry keys.

The malware are similar in that they utilized droppers that masquerade as installers for legitimate software applications like Adobe Reader, Juniper VPN, and Microsoft ActiveX Control. In some cases, a loading bar displays and then the user redirects to a login page for the associated software. The malware contain measures to avoid detection. The malware self-obfuscates as technology related applications such as media applications or VPN technologies. The malware establish persistence on the system, deploys remote access Trojans (RATs) such as the Derusbi malware, and features tools to record and seize user sessions. Tools such as PwDump and Scanline are included to steal user credentials, to allow the actor to escalate their privileges, to let the actor create unmonitored accounts, and to assist the attacker in lateral movements to systems across the network. Symantec believes that all three malware belong to the same family and that they have been updated and differentially developed over time by the same team. The malware is usually signed by the DTOPTOOLZ Co. signature belonging to a Korean software company. Domains and C2 servers often feature the names of Marvel comic book characters as the register [3].

Sandworm/ Quedagh/ BlackEnergy (Russian APT)

Sandworm has targeted governments and political organizations since at least 2009, but the group also may have been behind the 2008 cyber-attacks against Georgia. The Ukrainian government, NATO, the European Union, the European Telecommunications sector, European Energy companies, and the Polish government are among the group’s top targets. Attendees of the May 2014 Globesec conference were also targeted. Many of the decoy documents used to deploy the malware were spoofed news coverage of political or economic situations in Europe.

The BlackEnergy crimeware appeared for sale in underground Russian cyber-markets around 2007. The malware was designed to create botnets for Distributed Denial of Service attacks (DDoS), but it has since evolved to support other capabilities. BlackEnergy can create botnets to send spam emails for phishing campaigns, and it has tools to harvest passwords and banking credentials from infected computers.

The BlackEnergy toolkit gained notoriety during the 2008 cyber-attacks on Georgia during the conflict between Russia and Georgia. The BlackEnergy malware is available for purchase in cyber underground communities; however, the variant used in Sandworm attacks has been modified with custom code, incorporates a proxy server infrastructure, techniques to User Account Control and driver signing features in 64-bit Windows systems, and tools to collect documents. F-Secure notes BlackEnergy is used by a variety of criminal and cyber espionage groups; so, Sandworm’s adoption of BlackEnergy, instead of writing custom malware, may have been an attempt to evade attribution and blend into the crowd of nefarious actors to remain undiscovered.

Sandworm delivers malware through spear phishing emails containing a malicious document, such as a Microsoft PowerPoint attachment. The attachments either deliver the initial dropper or exploit a zero-day vulnerability to install the malware. In some cases, legitimate applications were trojanized to perform the installation. Through zero-day exploits, the malware infects any system running a Windows Operating System ranging from Vista to Windows, including Windows server systems. The malware only infects the victim system if the current user is a member of the local administrator group. If the user is not an administrator, then the malware will attempt to re-launch itself as Administrator or exploit the Windows backward compatibility features to bypass UAC.

The BlackEnergy toolkit features a builder application that generates the clients used to infect victim systems, server-side scripts to create C&C servers, and an interface for the attacker to communicate with their botnet. F-Secure comments that the toolkit is simple enough and convenient enough that anyone can build a botnet without possessing extensive skills. The information stealing plugin of the toolkit gathers system information, session information, a list of installed applications, a list of registered mail, browser, and instant messaging clients, a list of network connections, and stored user credentials for online and offline accounts, and exfiltrates the information back to the C&C server via a HTTP POST request. New variants of the malware may also be able to capture screenshots and record audio.

The current, third variant of the BlackEnergy malware, which is capable of stealing documents from targets, has been used against energy companies and government institutions in Ukraine and Eastern Europe. The initial appearance of the malware coincides with the conflict between Russia and Ukraine. Trend Micro discovered that the newest variant of the malware, customized by the group, can target ICS and SCADA systems. The group may have infected these systems to monitor or sabotage systems that compete with Russia’s energy interests.

On December 23, 2015, a Sandworm campaign against three Ukrainian power plants caused a severe outage using BlackEnergy3. The malware was delivered using spear phishing emails. The BlackEnergy3 malware disabled control system computers and forced shutdown of systems [4]. The attack required extensive reconnaissance and coordination between the attackers. According to company personnel, the cyber-attacks occurred within 30 minutes of each other and impacted multiple central and regional facilities. The attackers remotely disabled the breakers through a coordinated effort of multiple attackers who either utilized existing remote administration tools at the operating system level or exploited remote ICS client software via VPN connections. The companies believed that the attackers obtained legitimate credentials for each facility before the attack [5]. Power remained off until utility companies manually restored power. The malware features a wiper module called KillDisk that was used to disable both control and non-control system computers. At the same time, the attackers overwhelmed utility call centers with automated telephone calls, overloading the utilities' ability to receive outage reports from customers. Ukrainian power companies are not unique in their control systems. According to ICS-CERT, BlackEnergy3 has also been observed on United States, European, and other country's critical infrastructure systems as early as December 2014 [4].

Tarh Andishan/ Operation Cleaver (Iranian APT)

In December 2014, ICIT Fellow Cylance exposed Iranian threat actor, Tarh Andishan their Operation Cleaver investigation. Tarh Andishan may be a measured response to the Stuxnet, Duqu, and Flame campaigns. Alternatively, Iran may be attempting to enter into the global arena as a major cyber power, capable of competing with countries such as the United States, China, and Russia, in cyberspace. Cylance released Operation Cleaver early to allow potential targets the opportunity to mitigate the threat to their systems. Due to this decision, they estimate that they only discovered a portion of the activity of Tarh Andishan. Nevertheless, Cylance managed to build an impressive profile of Tarh Andishan's operation, including hacker profiles, domain names, internal infrastructure, and indicators of compromise.

Tarh Andishan's infrastructure has been traced to a defunct cooperation from which it earned its name. The infrastructure was hosted by an Iranian provider (Netafraz.com), and Autonomous System Networks (ASNs), IP source netblocks, and domains were registered in Iran. The netblocks utilized had strong associations to state-owned oil and gas companies that employ individuals with expert knowledge of ICS systems. Further, tools in the malware warn the attackers if their outward facing IP address traces back to Iran. The infrastructure utilized by the group is too robust and too centralized to have belonged to an individual or small "grass-roots" hacktivist group. This leads leading security firms, such as Cylance, to believe that Tarh Andishan is either state-sponsored or a well-funded mercenary hacker group.

Tarh Andishan consists of at least 20 dedicated hackers and developers, believed to be located in Tehran, Iran. Additional, members or hired associates operate out of the Netherlands, Canada, and the United Kingdom. Persian names (Salman Ghazikhani, Bahman Mohebbi, etc.) were used as hacker monikers. Most targets of Tarh Andishan speak English as a primary language, and it appears that members of the group are proficient in reading and writing in English. Different members of the group specialize in different malware, different malware development tools, different programming languages and different adversary techniques.

Tarh Andishan targets government entities and critical infrastructure facilities in Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States. Specifically, Tarh Andishan has been known to target: oil and gas facilities, energy facilities, utility facilities, military installations, transportation facilities, airlines, airports, hospitals, telecommunication companies, technology firms, institutions of education and research, aerospace and defense facilities, chemical companies, and governments. The high propensity for the group to target energy sector organizations indicates that Iran may be using the group to gain information about competitor organizations.

Tarh Andishan networked systems in South Korea, Saudi Arabia, and Pakistan by compromising Windows Active Directory and physical internal infrastructure such as Cisco edge switches, and routers. From there, the attackers stole VPN credentials so that they could establish a persistent presence and so that they could remotely access the entire infrastructure and supply chain. Tarh Andishan used the compromised credentials and VPN access to compromise physical systems, access security control systems, make fraudulent payments, and to infect other internal infrastructure.

According to Cylance, Tarh Andishan's "Initial compromise techniques include SQL injection, web attacks, and creative deception-based attacks – all of which have been implemented in the past by Chinese and Russian hacking teams." Tarh Andishan did not appear to utilize zero-day exploits. The SQL injection attacks were made possible by attacking vulnerable applications that failed to sanitize input before passing it to a database in an SQL query. Many Energy sector legacy systems remain vulnerable to known SQL injection vulnerabilities. Tarh Andishan had also used spear-phishing attacks when injection attacks failed. One such attack told targets that they had been selected to apply for a new position at an industrial conglomerate and the link directed them to a copy of a legitimate resume creation website. The resume tool was combined with a binder tool that loaded malware onto created documents. The malware runs in the background of the victim's system and logs keystrokes and the information entered into forms. After the malware infected a host, the attackers would leverage existing, publically available, exploits (such as MS08-067) to escalate their privileges on Windows systems. The malware then propagated through the network like a worm, to compromise other systems on the network. Tarh Andishan compromises Microsoft Windows web servers that run Internet Information Services (IIS) and Coldfusion, Apache servers with PHP, Microsoft Windows desktops, and Linux servers. The group also targets popular network infrastructure such as Cisco VPNs, Cisco switches, and routers.

Tarh Andishan's most utilized malware, TinyZBot, gathers information from infected systems and it establishes backdoors for persistent access. TinyZBot uses the SOAP sub-protocol of HTTP to communicate with the C&C infrastructure, and it abuses SMTP to exfiltrate data to the C&C servers. Among other capabilities, TinyZBot can also take screenshots of the system, download and execute arbitrary code, detect security software, disable some anti-virus, and modify PE resources. Once the malware has infected the system, Tarh Andishan can use customized tools to poison ARP caches, encrypt data, steal credentials, create backdoors, create ASP.Net shells, enumerate processes, record HTTP and SMB communications, detail the network environment, query Windows Management Instrumentation (WMI), log keystrokes, and more. Effectively, Tarh Andishan can customize their tools to suit any target. The Net Crawler tool, which combines popular attacker tools Windows Credential Editor, Mimikat, and PsExec, was used to gather the cached credentials from every accessible computer on the infected network. Shell Creator 2 was used to generate an ASPX web shell to protect the attacker from revealing internal information such as location by human error. The nbrute utility uses NMap to map the network and then it attempts to determine network credentials via brute force. The attackers can also use tools such as the PVZ bot tool to log keystrokes on specific botted systems and save information on infected systems to specific locations [3].

Patchwork/ Dropping Elephant/ Chinastrats (Cybercriminal)

The Patchwork APT discovered in December 2015, infected at least 2,500 victims in the seven months before its discovery. Evidence suggests that the group has been active since at least 2014. Patchwork targets government, energy, and other related organizations present in Southeast Asia and the South China Sea. Rather than develop their own malware or toolset, the APT uses copy-paste source code from GitHub and hacking forums. Patchwork could be state-sponsored; however, its lack of dedicated resources and its reliance on open source code, suggests that it may be a criminal organization. Patchwork is notably worrying because it proves that a group does not need to be sophisticated or original in order to be successful. The APT has been remarkably successful with only OSINT code and no 0-day vulnerabilities. Software patches would prevent most or all of the group's exploits, yet, a considerable number of victims were vulnerable.

The group spreads the hijacked malware through spear-phishing emails with titles related to China's activity in the South China Sea and that contain either PowerPoint attachments which exploit Sandworm's exploit (CVE-2014-4114) or CVE-201406352 or Word attachments that exploit CVE-2012-0158. Kaspersky Labs claims that the group uses watering hole attacks. The group also maintains social engineering Google+, Facebook, and Twitter accounts to draw people to watering hole attacks.

The group uses an assortment of multiple copy-pasted code from malware and malware kits such as Powersploit, Meterpreter, AutoIt, and UACME. Once the exploit compromises a system, Patchwork uses the open-source Meterpreter to carry out a reverse shell attack to gain total device access [6]. In some attacks, an UPX packed AutoIT executable is dropped, which in turn downloads additional components to facilitate document exfiltration. The amalgamated malware creates a backdoor that should have been easy to detect since most security software recognizes the underlying code. Nevertheless, the malware remained undiscovered until May 2016. The malware also searches the host for certain file types, If the malware detects valuable data, then it deploys a second-stage malware, also created from assorted pieces of code, which laterally searches the infected network for other hosts to infect.
Similar to MiniDuke or CommentCrew, the group hides its communications behind base64 encryption. Unlike either actor, Patchwork's encrypted data provides information about the next hop or the true C2 for the backdoor instead of initial commands.

The malware contains the time of day when the C2 servers were active and includes a list of Southeast Asian countries to target. Consequently, some security researchers believe the malware might originate in India or China [7] [8].

Potential of the SRS

No single lab, organization, or entity is solely responsible for securing the Energy sector, national security, or other critical infrastructure systems. DOE and DHS are tasked with the responsibility of securing the electric grid and other energy assets; however, the sector consists of a complex matrix of micro-grids and systems that are predominantly owned by private organizations that rely on public infrastructure. Complex regulatory challenges, technical obstacles, and ownership ambiguities further obfuscate and complicate the digital landscape surrounding assets that are frequently beleaguered by a variety of sophisticated and unsophisticated adversaries originating from multiple nations.

The Savanah River Site is ideally positioned and equipped to assist in the national security missions and the defense of the energy grid and other critical infrastructure assets. It could evolve to serve one or more of the following roles:

1) Secure Operations Center (SOC)
2) Vulnerability, Exploit, and Malware Clearinghouse
3) Cyber-kinetic Attack Emulation Site
4) Gamification and Emulation Site
5) Workforce Development Leader
6) Cyber-hygiene Educator
7) IT-OT Mitigation and Remediation Testing bed

Other Labs are Interested in Projects, Not Leadership Roles

Although research remains preliminary, other national laboratories have not indicated interest in committing their facilities to national security and critical infrastructure resiliency in the same manner as the Savannah River Site. In September 2017, the U.S. Department of Energy announced awards of up to $50 million to its national laboratories for early stage research and development of grid resiliency and cybersecurity tools. Over $20 million was earmarked for the creation of bleeding-edge tools and technologies to protect the United States' electric grid and oil and gas infrastructure from cyber threats. Another $30 million over three years was dedicated to DOE's Grid Modernization Laboratory Consortium to research resilient distribution systems, focusing on the integration of clean distributed energy resources, advanced controls, grid architecture, and emerging technologies at a regional scale. Argonne National Laboratory partnered with the Illinois Institute of Technology to research and develop a "cyber-attack-resilient architecture for next-generation electricity distribution systems that increase reliability by using distributed energy resources and microgrids." Lawrence Berkeley National Laboratory in California began investigating whether network defenders could enhance the resiliency of distribution grids via adaptive control algorithms for distributed resources and voltage regulation, or by analyzing attack scenarios and developing "associated defensive strategies." Idaho National Laboratory, Sandia National Laboratories in New Mexico, and Pacific Northwest National Laboratory in Washington are managing a $6.2 million three-year resiliency project entitled the "Resilient Alaskan Distribution System Improvements using Automation, Network Analysis, Control, and Energy Storage", or RADIANCE, that seeks to "enhance the resilience methods for distribution grids under harsh weather, cyber-threats, and dynamic grid conditions using multiple networked microgrids, energy storage, and early-stage grid technologies" [9].

The Department of Energy is Failing to Secure Critical Assets

The DOE developed a cyber-strategy in December 2015however it failed to create an implementation plan to facilitate policy, and as a result, entities remain uncertain on how to secure assets, respond to incidents, or repel cyber threats. In late 2017 the DOE's Office of Inspector General evaluated whether the agency's unclassified cybersecurity program provides proper protection for information systems operations and assets, as required by the Federal Information Security Modernization Act of 2014, and found the closure of 13 of the prior fiscal year's 16 weaknesses, and a reduction of nine vulnerability management findings in FY 2016 to five in FY 2017. Nevertheless, the report stressed that "issues related to vulnerability management, system integrity of web applications, and access controls continue to exist." For instance, at least three of the nearly one hundred DOE entities featured missing security patches, workstation and server software no longer supported by the vendor, or employed laptops, servers and workstations that were missing antivirus software updates that protected information system assets. One location's security program was unable to prevent malicious input data; if it were exploited, it could allow unauthorized access to the DOE's IT resources and enable attackers to compromise legitimate users' workstations and application login credentials.

Other issues persisted due to the DOE's failure to develop and implement their intended cybersecurity policies and procedures fully. As in prior fiscal year evaluations, the "current configuration and security patch processes" did not ensure that their cybersecurity remained current. Adequate risk and performance management programs, including security testing that ineffectively monitored IT programs at specific locations, were inconsistently implemented. Control weaknesses existed, such as a lack of adequately enforced identification and verification requirements and poorly implemented logging capabilities for monitoring user activities. As a result, some user accounts remained active for personnel no longer with the DOE, and 223 privileged users still had system access despite exceeding password expiration limitations [10].

If the lack of cybersecurity improvements perpetuates, particularly concerning enhanced controls and vulnerability management, then DOE's information systems' program will become increasingly vulnerable to "higher-than-necessary risk of compromise, loss and/or modification" by malicious adversaries. The OIG proffered 30 recommendations to programs and sites to help better the department's cybersecurity capabilities, including the need to address phishing and malware, continuous monitoring, multifactor authentication and PIV card implementation for local, remote and application access, among other areas of concern [10].

Available Funding Can Facilitate the SRS's Transition to Cybersecurity Leader

In February 2018, Energy Secretary Rick Perry announced the creation of the Office of Cybersecurity, Energy Security, and Emergency Response. The CESER office will focus on "energy infrastructure security," support the "expanded national security responsibilities" assigned to the DOE and will "enable more coordinated preparedness and response to natural and manmade threats." Proposed budgets suggested $96 million in funding to the office to bolster Energy sector cybersecurity. According to an October 2017 Accenture report, a global survey of utility executives concluded that 63 percent believe there is a moderate or significant risk of a cyber-attack on the electric grid in their country within the next five years. The new office intends to promote efforts to mitigate risks to the grid and remediate existing and known vulnerabilities [11].

In March 2018, the passage of the FY 2018 Omnibus bill secured the DOE $34.5 billion in funding. "As a former appropriator, I am keenly aware of the work that goes into the budget process, and I am grateful for the certainty that this FY 2018 Budget will bring our Department," remarked Secretary Perry. He continued, "This package funds our missions and will allow us to do great work for American energy. DOE will now be focused on executing our work under this budget in the most effective way possible" [12]. The package includes:

- $6.3 billion for Science research programs
- $2.3 billion for Energy Efficiency and Renewable Energy (EERE)
- $1.2 billion for Nuclear Energy
- $727 million for Fossil Energy
- $353 million for The Advanced Research Projects Agency-Energy (ARPA-E)
- $7.1 billion for Environmental Management (EM)
- $500+ million to advance exascale computing
- $100+ million for cybersecurity to protect electric grid and energy infrastructure

In April 2018, the DOE OE issued the INDUSTRY PARTNERSHIPS FOR CYBERSECURITY OF ENERGY DELIVERY SYSTEMS (CEDS) RESEARCH, DEVELOPMENT AND DEMONSTRATION Funding Opportunity Announcement which allocates $25,000,000 in federal funding towards projects that enhance the cybersecurity posture or advance information security research in the Energy sector.

Regional Synergies

The SRS facility is uniquely positioned to support additional information security missions related to securing critical infrastructure and safeguarding national security. The surrounding region is ideal for government, cybersecurity, and defense investment due to the synergies between the Savannah River Site, Fort Gordon, the CSRA Alliance, the NSA, and local higher education community. Many reputable defense contractors, healthcare organizations, and federal agencies already populate the area. Further, the Pentagon designated Fort Gordon as the new home of the Army's Cyber Command. Fort Gordon supports a population of 108,715 composed of 17,264 service members, 10,613 civilian employees, 22,450 family members, and 58,388 retirees. Technically, it is “the 6th largest city in Georgia”. Fort Gordon is the largest employer in the CSRA with an economic impact of $2.4B in FY17, with approximately $1.6B in payroll and the remaining $800M in construction, purchases and contracts, and federal impact aid to local school districts. Fort Gordon is the home of the Cyber Center of Excellence, composed of a Signal and Cyber School, 7th Signal Command (Theater), Joint Force Headquarters-Cyber (JFHQ-C), the Cyber Protection Brigade, several Intelligence & Security Command (INSCOM) Brigades, Dwight D Eisenhower Army Medical Center, the National Security Agency, and the US Army Garrison. The Alliance for Fort Gordon serves as a liaison between the greater Augusta/Aiken community and Fort Gordon, promoting economic development through business partnerships and advocating for improved quality of life for service members and their families. Moreover, as a result of the relocation of Cyber Command, before 2020 the area will see an influx of cybersecurity vendors and defense contractors with which talent can be exchanged and partnerships can be formed.

Additionally, many new startups and firms are supported by testbed and incubators affiliated with SRS, the CSRA Alliance, Fort Gordon, Augusta University, and the University of South Carolina Aiken. For instance, Governor Nathan Deal has committed more than $100 million to the development of the Hull McKnight Georgia Cyber Center for Innovation and Training. The center is a unique public-private partnership among academia, state and federal government, law enforcement, the U.S. Army, and the private sector. It is the most significant investment in a cybersecurity facility by a state government. The Cyber Center will promote continuous improvement in cybersecurity technology through education, training, research, and the development of practical applications to protect Georgia citizens. The center will create additional synergies between higher education, students, industry, and government. Further, the facility will provide a new cyber range to support the initiatives of agencies and partners [13].

Geography of the SRS

The SRS is ideally situated to support DOE's defense of the energy sector or the defense of other national security missions. Energy network and infrastructure surround the SRS. For instance, two nuclear power plants are located less than 75 miles away, and numerous other power plants and dams are nearby. The SRS covers 310 square miles (800 km^2) and employs more than 10,000 people. If the site pursues the adoption of critical infrastructure information security responsibilities, it can leverage ample existing facilities and available land to support the mission. Testing beds, cyber ranges, and cyber-kinetic models can be constructed, and discrete and invaluable tests can be conducted within the secure site. Currently, Fort Gordon contracts their existing cyber range on the installation. The Cyber Center of Excellence is located within the Greater Augusta/Aiken MSA Region supports the training, missions, and signal intelligence training of the US Army and other armed forces located at Fort Gordon. Through the partnership with the Hull McKnight Cyber Center for Innovation and Training, an additional cyber range is being developed. However, additional cyber ranges and SCIF facilities located on the SRS may be needed to accommodate long-term growth and promote national security missions. Through collaboration, higher education, other agencies, and the DOE can build off the existing and future successes at the SRS.

Low-Cost Development

Developing new missions at SRS maximizes the return on investment by leverage the low costs of development, capitalizing on the existing workforce, leveraging synergies with high education and industry partners like Fort Gordon and the US Army, and by attracting new talent to a region that is growing and offers a high quality of life. Very few places will offer the collective opportunities that are present in the area.

Community Engagement

Collaborative local leaders from government, academia, public service, businesses, and critical infrastructure engage with SRS, Fort Gordon, and the CDRA Alliance. They dedicate their time and attention to ensure that facilities and organizations, such as SRS, are successful in their missions because they recognize their necessity to the community. Through academic partnerships, related boards, and other opportunities, community leaders are dedicated to supporting SRS, Fort Gordon, and the CSRA Alliance. Workforce development, marketing, and the evolution of new missions are treated as regional priorities.

Economic Incentives will Draw Talent to the Region

Low cost of living and ample employment opportunities in niche critical infrastructure organizations may drive specialized talent to the region. The cost of homeownership in the area is more economical than many competing regions and could motivate millennials and other emerging workers to migrate around the SRS region. The climate, a vibrant art scene, ample outdoor recreation, and other communal attributes may be attractive to those looking to start or raise a family. Additionally, the SRS, USC Aiken, Augusta University, and Fort Gordon K-12 education initiatives improve the instruction of the local youth while fostering a capable future workforce dedicated to the greater region. Before the 2020 transition, Cyber Command will likely be seeking Software Developers, Electrical Engineers, Malware and Cyber-Forensic Analysts, Hardware Developers, Network Engineers, Data Analysts and Modelers, Cloud Engineers, and Big Data Architects.

The SRS

The Savannah River Site is dedicated to environmental stewardship, national security, and clean energy. It is accustomed to cleaning up the messes of the Energy Sector [14]. The sector is failing to secure its digital, information, and critical infrastructure resources. It is time for the SRS to adapt to serve as a central coordinating center for Energy sector information security. About half of the resources at SRS are dedicated to Environmental Management, while the rest support the National Nuclear Security Administration (NNSA) missions managed by the Savannah River Field Office. The IT and cybersecurity operations at SRS protect key mission priorities, defend the network from internal and external threats, intellectual property, national security assets, and the personal information of government personnel and contractors [14]. The site is uniquely positioned to ensure the confidentiality, integrity, availability, and resiliency of physical and digital energy sector critical infrastructure due to its proximity to Fort Gordon, its relationships with the region, its connections with defense and information security contractors, its associations with local academic institutions, and its developed resources and information security initiatives.

In August 2017, the Savannah River Remediation (SRR) team was named the champion October 2017's National Cyber Security Awareness Month for the third consecutive year. SRR earned the award for its strong cybersecurity culture and its role in the "STOP.THINK.CONNECT." global online safety awareness campaign. In 2014, SRR launched a user awareness program to educate its workforce on topics ranging from safe online shopping to secure online navigation. The creative cybersecurity education initiative was later shared with other sites across the DOE complex, and its cybersecurity perspective was related to students in Fort Gordon, Georgia [15].

In November 2017, the U.S. Department of Homeland Security, the National Cyber Security Alliance, and the National Cyber Security Awareness Month organization named the Savannah River Nuclear Solutions (SRNS) a champion of cyber security awareness for its efforts promoting a safer, more secure, and more trusted Internet. The SRNS provides cybersecurity and cyber-hygiene training for new personnel and annual refresher training for all employees. Ongoing cyber education and awareness activities are delivered through monthly safety meetings, pop-up messages on the site's intranet homepage, quarterly phishing exercises with follow-up training, and security roadshows and lunch and learn's throughout the year. Additionally, the SRNS sponsored a cyber education booth for the Science Education Enrichment Day for schoolchildren and supported the University of South Carolina Aiken cyber curriculum development and cyber lecture series [16].

Positives

- The SRS is situated and equipped for onsite and offsite cybersecurity missions.
- SRNL has a robust cybersecurity and cyber-hygiene reputation.
- The site has the space and facilities to host emulation and gamification exercises.

The SRS Could Lead Onsite and Offsite Cybersecurity Initiatives

The SRS is already secured against external and internal threats by physical, technological, and policy controls. A well-defined and defended security perimeter protects vital assets. The vast tracts of land onsite are well-suited for the isolated testing of wireless systems. Meanwhile, existing facilities could be repurposed to serve as a cyber works center similar in functionality and purpose to the Augusta Cyberworks sponsored by Cape Augusta, the University of Maryland Baltimore County Training Centers (UMBC TC), and the Augusta Warrior Project. For instance, building 703-A could be appropriated and secured for collaborative cybersecurity initiatives. 703-A is a 180,000 ft^2 DOE-owned building located within the property protected area of the site. Though it would require capital to rehabilitate, it could serve as a necessary site to facilitate the SRS cybersecurity mission. The building has already been the subject of SRNL rehabilitation studies, and it has potential as a candidate for historic preservation tax incentives or possible third-party investment.

Some SRS Information Security work could also be performed offsite in partnership with Fort Gordon, Augusta University, USC Aiken, the NSA Cyber Center, or other nationally reputable contractors and organizations. Interviews suggest that there is strong community support, ranging from individuals to businesses to elected officials, for collaborative cybersecurity work with SRS in the region. Federal delegations from both Georgia and South Carolina have expressed strong support for national security missions supported by SRS.

Cybersecurity is Already a Core SRNL Mission

Information systems used within SRS facilities meet all DOE and DHS modernization and security requirements, including compliance with NIST SP 800. Among its other assets, SRS already hosts real industrial process control systems working in secure environments with secure information. The SRNL already ensures the cybersecurity and resiliency of national security and Energy sector systems. For example, SRNL is a co-participant along with Clemson University and other industrial partners in the Wind Turbine Drive Train test facility in Charleston, South Carolina. SRNL staff capabilities include secure computing operations, and the lab operates national security programs and industrial cyber protection programs built to deter technology espionage. For instance, it can provide special wireless process and plant system security enhancements. SRS could collaborate with other regional cyber-range facilities (such as the Old King Mill in Augusta) to develop network protection capabilities.

The SRS Could Sponsor Emulation and Gamification Exercises

Physical SRS systems could be used to test grid protection technologies or to evaluate mitigation and remediation strategies in response to cyber-kinetic attacks. In fact, the vast open spaces and ample facilities within the SRS can be used to construct and operate test beds for electrical grid systems and components as well as niche system specific to other sectors, agencies, and organizations. Realistic to-scale tests are not as feasible at other sites. Additionally, the site could host comprehensive real-time gamification exercises in which other SRS personnel, agency staff, industry affiliates, or University students must evaluate, respond to, mitigate, and remediate a simulated incident that precisely mimics every layer of the actual tools, tactics, and procedures of sophisticated threat actors such as nation-state sponsored advanced persistent threat (APT) groups. Some of the results of these elaborate exercises are the training of critical infrastructure personnel, the development of meaningful incident response plans, and the deconstruction and analysis of adversarial attack patterns and behaviors.

The AMC Will Promote Cybersecurity Research among Regional Stakeholders

The Advanced Manufacturing Collaborative (AMC) is being developed through SRNL, sponsored by the U.S. Department of Energy, and located at USC Aiken. The AMC is a public-private partnership intended to be an innovation hub for manufacturing, fostering modern industrial practices, advancing new technologies and training the future manufacturing workforce with a focus on chemical and materials manufacturing. Core R&D areas include cybersecurity, smart manufacturing, robotics, virtual and augmented reality, and other topics. It combines the capabilities of DOE labs, such as SRNL, with industrial enterprises and educational institutions to drive innovation and sustained regional growth. Projected economic impacts of the AMC include $45 million in construction investments the generation of 200-400 temporary construction jobs and 110 permanent, high-wage R&D positions, and a focal point to draw additional economic development to the area. Further, the site could enrich the STEM awareness, including cybersecurity and cyber-hygiene topics, of 85,000+ local K-12 students [17]. AMC partners include:

- Aiken County Public Schools
- Aiken Technical College
- Augusta University
- BAE Systems
- BMW
- Boeing
- Bridgestone
- BWX Technologies, Inc.
- Clemson University
- Corning
- Dow
- Dupont
- Enercon Federal Services
- Fluor Corporation
- GE
- Greater Aiken Chamber of Commerce
- Guardian Manufacturing
- Materials Design, Inc.
- NanoTechLabs, Inc.
- Parsons
- Siemens
- Solvay
- South Carolina Jobs-Economic
- Development Authority
- South Carolina Small Business
- Development Centers
- South Carolina State University
- South Carolina Universities and
- Education Research Foundation
- University of South Carolina Aiken
- University of South Carolina

Workforce Development

Augusta University is an emerging national leader in cybersecurity education, and it is poised to play a pivotal role in training qualified talent to fill critical positions in public and private sector cybersecurity. It has been recognized as a National Center of Academic Excellence in Cyber Defense Education by the National Security Agency and the Department of Homeland Security. All signs indicate that Augusta University is and will continue to be a leader in cybersecurity education in the state and nation. It also signed a memorandum of understanding with the U.S. Army Cyber Center of Excellence to share resources and help develop a cyber-trained workforce through education, innovation, research, and outreach. The GenCyber camps offered through the Cyber Institute and funded through a grant from NSA and the National Science Foundation trains high school students in cyber defense. The annual Cyber Education Summit that brings together hundreds of government, industry and academic leaders to discuss the future of cybersecurity [18].

In February 2018, while on his first visit to both Savannah River Site and the Savannah River National Laboratory, U.S. Energy Secretary Rick Perry told more than 80 SRS and SRNL workers that cybersecurity is “the biggest challenge I’ve got” in the national security scope of his job. He continued that “The thing that I’m really most concerned about that’s in our wheelhouse (is) cybersecurity, and our ability to protect and defend this country. Statutorily, we’re the agency responsible for the electrical grid – and the protection of it, the resiliency of it, etc. Our national labs are obviously involved in concentric circles out from that, from the standpoint of cybersecurity, and working with other agencies in the government about how to defend our country against cyber attacks" [2].

There is a cybersecurity skill shortage of approximately 211,000 professionals. Veterans possess unique sets of skills, training, and discipline that makes them well suited for cybersecurity jobs. The Cyber Talent Vet Success Immersion Academy is an intense accelerated training program designed to provide transitioning veterans with a fast track to training, certifications, and employment in the cybersecurity industry. It is a collaboration between The Augusta Warrior Project, Augusta University Cyber Institute, and SANS Institute. The six-to-eight-week program is held at the Augusta University Cyber Institute, is free to qualified candidates, is valued at up to $30,000 per participant (depending on curriculum selected), and offers intense and immersive training for veterans interested in cybersecurity [19].

Positives

- Augusta University is affiliated with SRS and offers numerous cyber-related degrees
- USC Aiken is also affiliated with SRS and is improving its computer science, cybersecurity, and engineering degrees.
- Regional K-12 efforts will increase the cybersecurity workforce in the near future

Potential Deficiencies

- Some essential engineering programs are not offered at local universities.
- Risk analysis and quantification may need greater focus in university curriculums.

Augusta University

Augusta University invested approximately $6M in funding the development of cyber relevant programs over the last five years. Meanwhile, the state of Georgia invested over $100M in the Hull McKnight Georgia Cyber Center for Innovation and Training. The 165,000-square-foot facility will serve as an incubator hub for technology startups and offer training space for the state’s cybersecurity initiatives and workforce development programs. Partners in the Georgia Cyber Center include Augusta University, Augusta Technical College, the U.S. Army Cyber Center of Excellence at Fort Gordon, the Georgia National Guard, the Georgia Bureau of Investigation, the City of Augusta, the University System of Georgia, the Technical College System of Georgia, local school systems and private corporations [20].

Six percent (121) of the over 1,900 graduates from the university for the 2017-2018 academic year were in cybersecurity-related programs. Faculty anticipates a ten percent growth rate annually over the next five years, leading to approximately 200 graduates annually by the academic year 2022-2023. Through joint appointments, internships, recruitment fairs, and other outreach, many of these graduates could supply talent and expertise to the SRS and its evolving cybersecurity initiatives.

The Augusta Metro area is fertile for continued development and the evolution of cybersecurity and information technology initiatives which will require a growing qualified workforce. In 2017, Fortune magazine labeled the region as one of the cybersecurity capitals of the world [21]. The 2017 Augusta Metropolitan Area Cybersecurity Workforce Study recently conducted by Augusta University, found that cybersecurity will be one of the fastest growing areas of employment in the Augusta Metro area. The study's survey found that sampled businesses, nonprofits, and public agencies expect to grow their cyber and IT workforce by 138% over the next five years. According to the results of the survey, most employers in the region want their current and new employees to hold a bachelor's degree in information technology or computer science. Extrapolating this finding to all businesses, nonprofits, and public agencies means that the Augusta Metro cyber workforce may increase by over 4,000 positions, which will produce over an estimated $337 million in salary for the local economy. Because the region is an innovative hub for cyber- and information technology - related occupations, currently, over 5% [approximately 12,716 occupations] of the local workforce perform relevant roles. Further, on average, the jobs pay wages above national averages [22].

Augusta University offers an undergraduate cyber defense program of study that combines an IT or computer science degree with either a Cyber Defender Certificate or an Advanced Cyber Defender Certificate. Adults who have already earned degrees may apply for the Post-Baccalaureate earning cybersecurity certificate only program which allows them to retool and develop their cybersecurity expertise part-time over a two or three year period. Healthcare-oriented graduate students and professional healthcare workers can enroll in the two-semester Healthcare Information Security Graduate Certificate program. Meanwhile, students with existing academic or practical information technology experience can enroll in the graduate level Information Security Management (ISM) program to receive a four or five-semester graduate level management-oriented overview of the fields of information security, IT governance, and risk management. Additional relevant certificates include Certificate in Health Information Administration, Certificate in Cyber Crime, and Computer Science Endorsement (Certification for K-12 teachers). Bachelor degrees programs include Bachelor of Science in Computer Science (including the option to add a concentration in Cyber Operations), Bachelor of Science in Information Technology (including the option to add a concentration in Cybersecurity), Bachelor of Science in Health Information Administration, and Bachelor of Business Administration in Management Information Systems. The Master of Arts in Intelligence and Security Studies and Ph.D. and MS in Biostatistics programs are also available at the graduate level.

In addition to their existing programs, Augusta University will soon be launching a more extensive catalog of professional and continuing education courses. Several joint faculty appointments will be recruited from their business and industry partners to enable the university to respond to increased enrollment and program demand, while also providing students with internships and cooperative work assignments. As SRS is already among Augusta University’s partners, it is possible that SRNL or other cyber-focused staff could fill one or more of the appointments.

Augusta University plans to further develop their forensics program along with their Criminal Justice programs. If the curriculum includes cyber-forensics, coverage of Deep Web markets and forums, malware, ransomware, or other code, tools, procedures, and behaviors intrinsic to cyber threat actors, then graduates could prove useful hires in the SRS microcosm. Additionally, in the near future, Augusta University intends to offer Information Security Management Courses to all majors across the entire AU degree spectrum so that students in all disciplines will recognize their industry's Information Security risks and need to enhance security postures. In Fall 2019, the university will launch the Master of Science in Biological and Computational Mathematics program and the Master of Science in Data Science program featuring two concentrations, cybersecurity and genomics.

USC Aiken

The University of South Carolina Aiken plans to offer a Bachelor of Science in Mathematics/Computer Science degree with a concentration in cybersecurity. USC Aiken has a continuous relationship with SRS and SRNL. Staff from the SRS serve on the Engineering Advisory Board, adjunct teach courses every semester, and are connected to USC Aiken's degree development for cybersecurity and applied gaming, Students from USC Aiken seek internships and post-graduation employment at the SRS site. The university recognizes the importance of cybersecurity and cyber-hygiene; consequently, beginning in Fall 2018, it is splitting its combined math and computer science program into Bachelor of Science in Applied Mathematics and Bachelor of Science in Applied Computer Science, so that students can receive more focused training. The mutually beneficial transition will facilitate job placement for students and will diminish the talent shortage in the region. Moreover, the programs will be directly tailored to the cyber workforce in the Aiken area and will adapt to the evolving needs of the local stakeholders and employers [23].

Regional Technical Colleges Can Supplement the Workforce

A sizable workforce can be rapidly educated and trained for IT, network, and low-level security roles from local technical colleges. Aiken Technical College offers Associate degrees in Applied Science with an emphasis in Networking or an emphasis in Programming. The former learn hardware and software-specific concepts needed to install, maintain and troubleshoot complex interconnected business systems while the latter learn knowledge and skills in programming languages and applications required to create, manage, and troubleshoot software systems and websites for businesses. The college also offers a certificate in Computer Networking and an Associate in Applied Science with a focus in Network Systems Management. Students with prior technical experience or training can receive credit for a combination of approved military training courses, Aiken Technical College online courses, and industry-recognized Information Technology certifications that align with the degree [24]. Similarly, Augusta Technical College offers Associate of Applied Science degrees in Cybersecurity and numerous computer programming languages, Cisco and Microsoft networks, Web Interface Design, and other Information Technology topics [25].

Augusta University and USC Aiken Lack Some Engineering Programs

At the moment, Augusta University and USC Aiken do not prominently feature specialized programs dedicated to Network Security, Software Engineering, Application Development, Systems Engineering, or similar degrees. Personnel specializing in these fields help to develop secure applications, reverse engineer malware, implement, manage, and configure some IT-OT infrastructure in accordance with the Information Security team, and otherwise assist in ensuring that the confidentiality, availability, and integrity of critical systems and sensitive data remain uncompromised.

Despite the deficiency in specialized degrees, USC Aiken does offer courses focused on software engineering, multiple programming languages, application development, algorithmic design, mobile computing, operating systems, database programming, and other related topics. USC Aiken also offers a Bachelor of Science in Industrial Process Engineering which could prove useful in combination with cybersecurity training [26]. Within five years, Augusta University intends to develop engineering degrees related to cybersecurity to assist the development and growth of the region's cybersecurity industry base. They also plan to develop a more technical master's degree program that will eventually lead to Ph.D. programs in Secure Software Engineering and Secure Systems Engineering. Joint appointments and SRNL staff could help shape the emerging workforce by proffering feedback on proposed curriculum and guidance on emerging needs in realistic national security and critical infrastructure environments.

Risk Analysis and Quantification

Information Security education is most effective when courses provide a multidisciplinary approach that imbues students with a multi-stakeholder viewpoint to problem-solving, incident response, and emerging threats. Risk-based analysis, communication skills, and the ability to quantify risk are vital to the success of the cybersecurity workforce. Further examination of the curriculum offered at Augusta University, and USC Aiken is necessary to determine whether these skills are transferred. If not, SRS faculty who act as adjuncts or personnel with extensive knowledge may advise the universities on how to best adapt their course offerings to fulfill the needs of local organizations.

A Continuous Workforce is Generated by Cybersecurity Education Initiatives

Augusta University, USC Aiken, Fort Gordon, and SRS sponsor and support K-12 education initiatives that increase cybersecurity and cyber-hygiene awareness and increase the likelihood that students will pursue higher education in Information Security fields. In the near to long-term future, education efforts could mitigate the cyber talent shortage and help to de-escalate the asymmetric threat landscape surrounding critical infrastructure systems by improving incident response, decreasing the incidence of insider threat and social engineering successes, and normalizing cyber-hygiene and security-by-design. For instance, Augusta University, along with the Aiken Technical College, the Augusta Metro Chamber of Commerce, Augusta Technical College, the CSRA Alliance, the Columbia County Chamber of Commerce, the Columbia County School System, Fort Gordon, and the Richmond County School System, developed the Alliance for CyberSecurity Education (ACE) to raise the effective value of the secondary educational system’s cyber education and its integration into post-secondary education. The initiative advances area students’ capabilities, generates an employable workforce for regional organizations, and positions the CSRA as a resource and partner with NSA-Georgia, Cyber COE and Fort Gordon in cybersecurity expertise.

Conclusion

Funding for the cybersecurity development of the SRS is available through the DOE, and no other national labs have proposed cybersecurity leadership roles similar to what SRS can provide. The Savannah River Site is unique in its proximity to national security entities, critical infrastructure organizations, leading academic institutions, and reputable defense and healthcare organizations. The site already has the facilities, assets, and culture necessary to be a cybersecurity leader. An ample workforce is available and continues to grow. Meanwhile, the stability and economic growth of the region suggest that recruiting talent from outside the area will not be a problem if necessary. Overall, elevation to a cybersecurity authority and leader appears a natural transition for the SRS and would incite considerable economic growth in the region.

Sources

[1]"East Georgia Fast Becoming Hub for US Cybersecurity Efforts", *US News*, 2017. [Online]. Available: https://www.usnews.com/news/best-states/georgia/articles/2017-08-05/east-georgia-fast-becoming-hub-for-us-cybersecurity-efforts. [Accessed: 22- May- 2018].

[2]J. Hotchkiss, "In first SRS visit, Perry raises issue of cybersecurity - The Augusta Chronicle, 2018-02-03", *Digital.olivesoftware.com*, 2018. [Online]. Available: http://digital.olivesoftware.com/Olive/ODN/AugustaChronicle/shared/ShowArticle.aspx?doc=TAC%2F2018%2F02%2F03&entity=Ar00101&sk=73551428&mode=text. [Accessed: 22- May- 2018].

[3] Cyber Attacks On The Ukrainian Grid: What You Should Know. 1st ed. FireEye, 2016. Web. 9 Aug. 2016. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

[4] Leyden, John. "Blackenergy Malware Activity Spiked In Runup To Ukraine Power Grid Takedown." Theregister.co.uk. N.p., 2016. Web. 9 Aug. 2016. http://www.theregister.co.uk/2016/03/04/ukraine_blackenergy_confirmation/

[5] "The Dropping Elephant Actor - Securelist." Securelist.com. N.p., 2016. Web. 9 Aug. 2016. https://securelist.com/blog/research/75328/the-dropping-elephant-actor/.

[6] Daily Open Source Infrastructure Report 11 July 2016. 1st ed. DHS, 2016. Web. 9 Aug. 2016. https://www.dhs.gov/sites/default/files/publications/dhs-daily-report-2016-07-11.pdf

[7] Operation SMN. 1st ed. Novetta, 2016. Web. 9 Aug. 2016. http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

[8] Operation SMN. 1st ed. Novetta, 2016. Web. 9 Aug. 2016. http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf

[9] "Energy Department Invests Up to $50 Million to Improve the Resilience and Security of the Nation’s Critical Energy Infrastructure", *Energy.gov*, 2018. [Online]. Available: https://www.energy.gov/articles/energy-department-invests-50-million-improve-resilience-and-security-nation-s-critical. [Accessed: 26- May- 2018].

[10] "Evaluation Report: DOE-OIG-18-01 | Department of Energy", *Energy.gov*, 2018. [Online]. Available: https://www.energy.gov/ig/downloads/evaluation-report-doe-oig-18-01. [Accessed: 26- May- 2018].

[11] J. Pyper, "DOE Forms a New Office Dedicated to ‘Energy Infrastructure Security’", *Greentechmedia.com*, 2018. [Online]. Available:

https://www.greentechmedia.com/articles/read/doe-new-office-energy-infrastructure-security-cybersecurity. [Accessed: 26- May- 2018].

[12] "DOE Hails Passage of FY 2018 Omnibus Bill", *Energy.gov*, 2018. [Online]. Available: https://www.energy.gov/articles/doe-hails-passage-fy-2018-omnibus-bill. [Accessed: 26- May- 2018].

[13]"Hull McKnight Georgia Cyber Center for Innovation and Training", *Georgia.gov*, 2018. [Online]. Available: https://georgia.gov/agencies/hull-mcknight-georgia-cyber-center-innovation-and-training. [Accessed: 22- May- 2018].

[14]"Chief Information Officer Talks Savannah River Site Cybersecurity with Army School", *Energy.gov*, 2016. [Online]. Available: https://www.energy.gov/em/articles/chief-information-officer-talks-savannah-river-site-cybersecurity-army-school. [Accessed: 22- May- 2018].

[15]"Officials Recognize SRS Contractor Cybersecurity Team's Capabilities", *Energy.gov*, 2017. [Online]. Available: https://www.energy.gov/em/articles/officials-recognize-srs-contractor-cybersecurity-team-s-capabilities. [Accessed: 22- May- 2018].

[16]"SRS Contractor is Cyber Security Awareness Champion", *Energy.gov*, 2017. [Online]. Available: https://www.energy.gov/em/articles/srs-contractor-cyber-security-awareness-champion. [Accessed: 22- May- 2018].

[17] "Working with SRNL - The Advanced Manufacturing Collaborative", *Srnl.doe.gov*, 2018. [Online]. Available: https://srnl.doe.gov/amc/index.htm. [Accessed: 26- May- 2018].

[18]G. Kauffman, "AU Cyber Institute Gains National Recognition | Buzz On Biz", *Buzzon.biz*, 2016. [Online]. Available: http://buzzon.biz/2016/06/au-cyber-institute-gains-national-recognition/. [Accessed: 22- May- 2018].

[19]K. Courtesy, "Free cyber training available for veterans | January 8, 2016 | www.fortgordonglobe.com | Fort Gordon Globe", *Fortgordonglobe.com*, 2018. [Online]. Available: http://www.fortgordonglobe.com/news/2016-01-08/News_Update/Free_cyber_training_available_for_veterans.html. [Accessed: 22- May- 2018].

[20]"Groundbreaking ceremony held for Georgia Cyber Center for Innovation and Training expansion", *Jagwire*, 2018. [Online]. Available: https://jagwire.augusta.edu/archives/50185. [Accessed: 22- May- 2018].

[21]J. Roberts, "7 Cities Vying to Be the World's Cybersecurity Capital", *Fortune*, 2017. [Online]. Available: http://fortune.com/2017/04/06/cyber-security-cities/. [Accessed: 22- May- 2018].

[22]"Cyber Institute | MPA Cybersecurity Workforce Study", *Augusta.edu*, 2018. [Online]. Available: http://www.augusta.edu/pamplin/mpa/documents/2017_augusta_metro_cybersecurity_workforce_study.pdf. [Accessed: 22- May- 2018].

[23] M. Kaufax, "USCA Getting with the Cyber Program", *Wrdw.com*, 2017. [Online]. Available: http://www.wrdw.com/content/news/USCA-Getting-with-the-Cyber-Program-441692853.html. [Accessed: 26- May- 2018].

[24] "Aiken Technical College", *Atc.edu*, 2018. [Online]. Available: https://www.atc.edu/. [Accessed: 26- May- 2018].

[25] "Home - Augusta Technical College", *Augustatech.edu*, 2018. [Online]. Available: https://www.augustatech.edu/. [Accessed: 26- May- 2018].

[26]"Engineering Programs | Engineering | USC Aiken", *Usca.edu*, 2018. [Online]. Available: https://www.usca.edu/math/academics/engineering/. [Accessed: 22- May- 2018].