ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

# The Cyber X Factor of the Savannah River Site

## An Assessment of the Potential for the Savannah River Site Region to Address our Nation's Cybersecurity & Resiliency Needs

**September 2018**

**Authored by:**

**Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology**

**Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology**

# The Cyber X Factor of the Savannah River Site

## An Assessment of the Potential for the Savannah River Site Region to Address our Nation's Cybersecurity & Resiliency Needs

**September 2018**

Authored by

Parham Eftekhari, Executive Director, Institute for Critical Infrastructure Technology

Drew Spaniel, Lead Researcher, Institute for Critical Infrastructure Technology



ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

**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 arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Our mission is to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

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 policy makers, 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

Executive Summary ..... 4
Introduction ..... 5
About the Savannah River Site ..... 5
Fort Gordon ..... 5
Savannah River National Laboratory (SRNL) ..... 6
The SRS Is Cyber-Ready: Facilities, Talent, Community ..... 6
Ample Facilities ..... 6
Strong Collaborative Community Ties ..... 7
A Security-Aware Workforce ..... 7
The SRS Incubator: The Potential Is Endless ..... 7
Defense of Energy and Other Critical Infrastructure ..... 8
Cyber First Response ..... 8
Vulnerability, Exploit, and Malware Clearinghouse ..... 8
Secure Operations Center (SOC) ..... 8
Cyber-Kinetic Attack Emulation Site ..... 8
IT-OT Mitigation and Remediation Testing Bed ..... 9
Gamification and Emulation Site ..... 9
Workforce Development Leader ..... 9
Cyber-Hygiene Educator ..... 9
The Energy Sector Needs the SRS ..... 10
Regional Synergies ..... 10
Collaborative Initiatives Are Available in the SRS Impact Area ..... 11
A Vibrant and Attractive Quality of Life ..... 12
The SRS Region Offers a High Quality of Life at Low Costs ..... 12
Grassroots Security Community ..... 12
Ample Lucrative Opportunities for a Growing Workforce ..... 12
Conclusion: The SRS Is the Ideal Site for Critical Infrastructure Cybersecurity Missions ..... 13

## Executive Summary

The Savannah River Site (SRS) is ideally positioned and equipped to assist in national security missions and defense of the electric grid and other critical infrastructure assets and is poised to emerge as a major national cybersecurity hub.

- The SRS houses the Savannah River National Laboratory (SRNL) and is near Fort Gordon, which will be the permanent home of the U.S. Army Cyber Command as of 2020.

- The SRS features ample facilities with strong security ingress and egress; has strong ties to local agencies, facilities, and communities; and is surrounded and staffed by a growing security-aware workforce that has demonstrated commendable cybersecurity and cyber-hygiene practices.

- Opportunities for existing facilities in the SRS include a cybersecurity first response, a vulnerability clearinghouse, a testing and emulation site, a centralized cybersecurity hub or Security Operations Center (SOC), or any number of roles and capacities supporting national security and critical infrastructure resiliency.

- An SRS-based initiative would be able to leverage the unique synergies that exist between Fort Gordon, SRNL, and local higher education institutions in order to combat the hyper-evolving threat landscape, address the developing needs of national critical infrastructure, and promote cybersecurity and cyber-hygiene training and awareness.

- Local area partnerships are available with national security entities, critical infrastructure organizations, leading academic institutions, and reputable defense and healthcare organizations.

- The SRS is a welcoming, vibrant, and economically thriving region, rife with unparalleled development opportunities and featuring a low cost of living for a high quality of life.

Failing to empower the SRS to reach its potential as a national cybersecurity leader and operational center would be a missed opportunity for our nation. The SRS is the cybersecurity steward that the Energy sector desperately needs, and it is ideally positioned to fulfill that role, as well as to assist in the national security and the resiliency of other critical infrastructures.

## Introduction

The nation's democratic institutions and critical infrastructure sectors, such as Energy, Healthcare, Finance, Manufacturing, and Government, are under attack. Both private and public sector leaders are frantically searching for environments where national security innovators can collaborate to create and execute the cybersecurity defenses needed to protect our most valued assets. The Savannah River Site (SRS) is unparalleled in its potential to offer a solution and act as a multi-disciplinary, stakeholder-driven Information Security Hub, thanks to its regional synergies; collaborative initiatives; low development costs; academic partnerships; and an evolving intelligence, defense, and critical infrastructure community.

By 2020, the U.S. Army Cyber Command will transfer to Fort Gordon, bringing with it unparalleled technological, political, and economic influence to the region. Additionally, the new $95 million Hull McKnight Georgia Cyber Innovation and Training Center in downtown Augusta, Georgia, on Reynolds Street will be the centerpiece of cyber activity in the region. Perhaps even more important is the passion of local and state leaders who understand the contributions the SRS can make to national security and these cyber initiatives.

With these capabilities, the cybersecurity leadership possibilities for the SRS are endless. Could it be the home to a Cyber National Guard or first responder unit to protect critical infrastructure? A Security Operations Center (SOC) or vulnerability clearinghouse? A testing bed and emulation site? The centralized location for Energy sector or other public/private sector cybersecurity activities?

While further research is needed to determine the path that will drive the best outcomes for the nation, the message is clear: the Savannah River Site is positioned to improve the cybersecurity posture of the nation in myriad ways. The only remaining question is who will seize upon this remarkable opportunity?

## About the Savannah River Site

Since its establishment in the early 1950s, the Savannah River Site has been a key economic driver in Aiken, Barnwell, and Allendale counties in South Carolina, and in Richmond and Columbia counties in Georgia. The SRS site covers 310 square miles near Aiken, South Carolina; however, the SRS Impact Area extends into five counties. The Savannah River Site is home to the Savannah River National Laboratory, and it is near Fort Gordon, both of which are vital to national security and pacesetters in the field of cybersecurity.

### Fort Gordon

Fort Gordon is home to the U.S. Army Cyber Center of Excellence and host to a multiservice community of Army, Marines, Navy, Air Force, Coast Guard, and multinational forces. It has become a center for joint forces activities, training, and operations. The U.S. Army Cyber Center of Excellence at Fort Gordon employs 30,000 military and civilian personnel and currently has an estimated $1.1 billion economic impact on the Augusta-Richmond County economy. The site is invaluable to national security, and its significance will increase by the 2020 transition.

Fort Gordon currently houses Signal Intelligence, Cyber Security, Surveillance, Reconnaissance, Military Intelligence, and cyber training facilities for the United States Army. The National Security Agency and Central Security Service also have a joint service command on the premise. Additionally, the Navy and Marine Corps operate units on the site. Fort Gordon also houses the Headquarters for the United States Army Cyber School and the Signal School. The Cyber School instructs soldiers on both offensive (disabling enemy networks is one potential tactic) and defensive cybersecurity (such as trying to find vulnerabilities in U.S. military systems before an adversary can). The Signal School focuses on communications technology that the United States Army is currently utilizing. The Signal School is currently training Signal Support System Specialists, who perform both signal and cyber-related duties.

### Savannah River National Laboratory (SRNL)

SRNL is the newest of all the National Laboratories and the only laboratory under DOE's Environmental Management purview. SRNL is renowned for its cybersecurity, cyber-hygiene, and educational initiatives. As a result, it is uniquely positioned to meet current and future energy and national security challenges and missions.

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. For example, SRNL is the FBI "Hub Lab" for pre-detonation forensics. The laboratory currently serves the nation in three major program areas:

1) National and Homeland Security
2) Energy Security
3) Environmental and Chemical Process Technology

## The SRS Is Cyber-Ready: Facilities, Talent, Community

### Ample Facilities

The work of the Energy sector, Intelligence Community, and other critical infrastructure stakeholders is sensitive. It necessitates secure facilities that are isolated from potential threats. With layered physical, technological, and policy-based controls, the Savannah River Site is already designed to be protected against internal, external and digital threats. The site covers a massive 310 square miles that are ideal for hosting and developing security operations centers, training facilities, testbed facilities, collaboration sites, and IT-OT tests. Entire buildings at the SRS remain empty, awaiting meaningful employment and revitalization. For instance, building 703-A is a 180,000-square-foot, DOE-owned building located within the secured area of the site that could be appropriated and secured for any number of collaborative cybersecurity initiatives. 703-A has already been the subject of SRNL rehabilitation studies, and it could be a potential candidate for historic preservation tax incentives or possible third-party investment. Ample space is also available for facilities to be constructed as necessary.

### Strong Collaborative Community Ties

Through collaboration with Fort Gordon; Augusta University; USC Aiken; local technical colleges; and other strategic partners, agencies, and nationally reputable organizations, innovative information security and other research and development projects could also be conducted at off-site facilities local to the SRS. Strong support from elected officials, businesses, and regional partners suggests that the site is positioned in what could be the next "Silicon Valley of Information Security and Innovation." No other region matches the collaborative opportunities currently present in the area.

### A Security-Aware Workforce

Developing new initiatives in the SRS region capitalizes on the stable economy, low development costs, and growing workforce of the area while minimizing the cost to establish mission-critical sites and facilities. Because SRS staff already consider Information Security and cyber-hygiene a top priority, hosting facilities in the region would not incur the workforce development costs posed by other sites. In fact, the staff at the Savannah River Site actively promote cybersecurity awareness and training in the surrounding area, which ensures that the future workforce will be likewise prepared to face the threat landscape. For example, in 2014, the Savannah River Remediation (SRR) team 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. In August 2017, the Savannah River Remediation (SRR) team was named the champion of 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 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 cybersecurity 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.

## The SRS Incubator: The Potential Is Endless

The 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. One or more development opportunities at the site could be pursued to rectify national deficiencies and fulfill a number of growing critical infrastructure needs.

## Defense of Energy and Other Critical Infrastructure

The personnel at the SRNL are renowned for their cybersecurity knowledge. Rather than each firm in the sector managing the security settings and controls applied to their systems and networks, the experienced staff of the SRS could manage the defense of the sector and ensure that adversaries are not able to breach sensitive networks because of mismanagement or gaps in security layers.

## Cyber First Response

Too many organizations do not adequately or correctly respond to cyber incidents in real time. The pressure and lack of experience often contribute to haphazard decisions that amplify the negative impacts of the breach and result in significantly greater damage and harm. For the most part, critical infrastructure organizations receive limited assistance in the event of an attack. For many, all they can do is rely on the responses and actions of third-party vendors and law enforcement. Instead, the SRS is ready and willing to serve as a Cyber First Response unit or house a Cyber National Guard that can be physically or digitally deployed to the site of a cyber incident, where it can coordinate mitigation and remediation efforts with expertise and rational judgment.

## Vulnerability, Exploit, and Malware Clearinghouse

The SRS could serve as a clearinghouse for indicators of compromise and other technical markers that can be used to detect, characterize, identify, profile, and mitigate threats. Trends in data or patterns in attacks could help to identify attacks as or before they occur, and potential victims may be notified with enough time to strengthen their defenses and mitigate the attacks. The SRS has numerous collaborative partnerships that it can leverage to collect valuable intelligence data, ranging from threat profiles to technical indicators that can be used to defend systems that are vital to national security.

## Secure Operations Center (SOC)

Secure Operations Centers house an information security team that is tasked with continuously monitoring and analyzing an organization's security posture. The team detects, analyzes, and responds to cybersecurity incidents in near-real time, using practiced processes and technical controls. The SRS could develop an SOC that monitors, analyzes, and protects Energy sector and other critical infrastructure from digital threats.

## Cyber-Kinetic Attack Emulation Site

Cyber-kinetic attacks, in which an adversary deploys malware to cause physical damage to a remote system, are on the rise. Using malware that is already outdated, attackers can wipe systems, disable safety controls, or even cause minor explosions or pipeline spills. While some of the defense against these attacks can be done from a computer or virtual machine, invaluable insight into the methodology of a threat actor and the anatomy of an attack can only truly be gained through physical emulation of a possible attack. Most facilities lack the space to stage tests on large Energy equipment; however, the SRS has ample knowledgeable staff, space, and security to stage sensitive tests and evaluate the intricacies of potential attacks.

## IT-OT Mitigation and Remediation Testing Bed

Organizations are only just beginning to recognize the significance in differing their approaches to the security of integrated information technology (IT) systems and operational technology (OT) systems. Threats to IT-OT networks are complex and not as well understood as other attack profiles. At the SRS, IT-OT networks could be emulated, attack methodologies could be analyzed, and security solutions could be tested and developed.

## Gamification and Emulation Site

Similarly, the SRS can help to develop or host gamification exercises that are designed to train staff ranging from clerical interns to security personnel in cyber-hygiene, incident response, and other best practices. Staff at the SRS actively research gamification and collaborate with local higher education institutions.

## Workforce Development Leader

The SRS is well-known for its exceptional cyber-hygiene and cybersecurity training initiatives. It stands as a role model for other labs and regional partners to imitate. In the future, the SRS could leverage its collaboration with local initiatives, education institutions, businesses, and agencies in programs and partnerships meant to educate and train current personnel and fresh talent in cyber-hygiene and cybersecurity best practices. Training could be tailored to the needs of the organization and their position in the fabric of national security. By helping to develop a widespread workforce that automatically adheres to best practices, the SRS could galvanize a renaissance in cybersecurity and cyber-hygiene. Perhaps in the future, humans might no longer be the weakest link in the security perimeter. Maybe adversarial compromise would no longer be a guarantee. The SRS is already actively improving national security via workforce development in its K-12 and higher education initiatives in the region.

Currently, there is a shortage of 211,000 cybersecurity professionals in the national workforce, and the need for well-educated skilled cyber professionals is likely to increase drastically as Artificial Intelligence, the Internet of Things, and other technologies continue to develop at an unparalleled pace. Through its partnerships with government entities and regional educational institutions, the SRS could help to train professionals rapidly. For instance, veterans possess unique skill sets, training, and discipline that make them well-suited for cybersecurity jobs. Augusta University, a regular partner with the SRS, has collaborated with The Augusta Warrior Project and SANS Institute to offer the Cyber Talent Vet Success Immersion Academy, an intense accelerated training program designed to provide transitioning veterans with a fast track to training, certifications, and employment in the cybersecurity industry. The SRS could collaborate with Augusta University, Fort Gordon, or a number of other partners to initiate workforce training initiatives that improve the cyber posture of organizations across the country.

## Cyber-Hygiene Educator

With additional attention, interest, and capital, the award-winning SRS staff could share their cyber-hygiene education materials with firms, personnel, and students located anywhere in the nation.

## The Energy Sector Needs the SRS

In the modern digital age, everything depends on energy. Without electricity, even simple operations in businesses, homes, hospitals, and government agencies grind to a sudden halt. The electric grid is so essential to everyday life that it is the only critical infrastructure network that is visible in every state, city, and home across the nation. Citizens depend on it so much that most take it for granted; like air, it is assumed so pervasively present that most do not think about it unless it is suddenly not available. Only during a power failure, when control over temperature management, entertainment, cooking, refrigeration, light, and services is 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 cyber threat actors because it is the backbone of the nation, yet the security of Energy assets and other critical infrastructure remains subpar, because of the shortage of firms equipped to address the challenges facing the sector holistically.

While a malware campaign cannot take down the entire grid, a dedicated adversary can impact targeted regions and inflict significant harm through disruption of energy delivery, via cyber-kinetic attacks on vital systems, or through the unauthorized alteration of critical data. Repairs to Energy systems are expensive. Every minute that electricity delivery is disrupted costs money and lives.

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 responsible for 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. As a result of the complexities of the sector, major security deficiencies exist. Multi-faceted facilities capable of adapting to counter the threats posed by the hyper-evolving digital landscape are rare. The Savannah River Site is ideally positioned and equipped to assist in the national security missions and the defense of the electric grid and other critical infrastructure assets.

## Regional Synergies

The SRS is ideally situated to support DOE's defense of the Energy sector or the defense of other national security missions. By 2020, Army Cyber Command will fully relocate to Fort Gordon. Countless critical infrastructure facilities, federal contractors, innovative education institutions, and agencies are also within a short drive of the SRS. The region is ideal for government, cybersecurity, and defense investment because of the synergies between the Savannah River Site, Fort Gordon, the CSRA Alliance for Fort Gordon, the NSA, and the local higher education community. Many reputable defense contractors, healthcare organizations, and federal agencies already populate the area. Moreover, as a result of the relocation of Cyber

Command, before and after 2020, the area will see an influx of cybersecurity vendors and defense contractors which can exchange talent and form partnerships. Additionally, many new startups and firms are supported by testbed and incubators affiliated with SRS, Fort Gordon, the CSRA Alliance for Fort Gordon, Augusta University, the University of South Carolina Aiken and local technical colleges. For instance, Governor Nathan Deal has committed more than $95 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. Furthermore, the facility will provide a new cyber range to support the initiatives of agencies and partners.

## Collaborative Initiatives Are Available in the SRS Impact Area

Opportunities to develop collaborative multi-stakeholder initiatives that address cybersecurity challenges are available in the region. Within the SRS Impact area, stakeholders have invested their attention, capital, expertise, time, and other resources to combating cyber threats, because the organizations and individuals in the SRS region genuinely care about improving national security. By leveraging its extensive network of collaborators, agency partners, affiliated labs, and other associations, the SRS can increase regional commitment to enhancing the national cyber posture and catalyze creative collaborative solutions for critical infrastructure and intelligence networks.

The Advanced Manufacturing Collaborative (AMC) is being considered by SRNL, sponsored by the U.S. Department of Energy, and located at USC Aiken. The AMC is a planned 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 research and development (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, a generation of 200 to 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 more than 85,000 local K-12 students.

Meanwhile, the state of Georgia invested over $95 million 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.

## A Vibrant and Attractive Quality of Life

### The SRS Region Offers a High Quality of Life at Low Costs

The SRS region offers a high quality of life, a stable and growing economy, and ample employment opportunities in both the public and private sectors. In 2017, Fortune magazine labeled the region as one of the cybersecurity capitals of the world. Because the region is an innovative hub, over 5 percent of the current workforce [approximately 12,716 individuals] work in cybersecurity and information technology occupations for salaries that are approximately double the local and national gross incomes, on average. As a result, cyber professionals in the region can afford a higher quality of life than in some other parts of the country.

### Grassroots Security Community

The region is attractive to new talent interested in starting a family. The cost of homeownership in the area is more economical than many competing regions and could motivate millennials and other emerging workers to migrate to 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.

### Ample Lucrative Opportunities for a Growing Workforce

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 percent over the next five years. The Augusta metro cyber workforce may increase by over 4,000 positions, which will produce more than $337 million in estimated wages for the local economy. Degrees prerequisite to meet the needs of local businesses can be obtained at regional education institutions. Further, by 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.

## Conclusion: The SRS Is the Ideal Site for Critical Infrastructure Cybersecurity Missions

The SRS region is ideally positioned and equipped to assist in the national security missions and the defense of the electric grid and other critical Energy infrastructure assets, thanks to unique regional synergies, unparalleled collaborative opportunities, a growing local workforce, a site with strong security ingress/egress and significant landmass to host numerous cyber-related exercises and demonstration projects, and a stable economy that allows for a high quality of life and a low cost of living within a vibrant community that continues to evolve because of low development costs.

Policymakers, national security leaders, cybersecurity technology providers, and critical infrastructure owner/operators should immediately investigate the untapped resources that exist in the SRS region and capitalize on these opportunities, ultimately benefiting the nation from an economic, Energy sector, and national security perspective.

**Authors Note:** The findings in this publication represent a summary of a larger and more in-depth research study conducted by ICIT entitled "The Cybersecurity Potential of the Savannah River Site," published in June, 2018. If you are interested in receiving a copy of that report, please contact ICIT.

# ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

**ICIT Websites & Social Media**

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-