Critical Infrastructure Security and Resilience Research, Development, Test, and Evaluation Spend Plan

April 25, 2022

Fiscal Year 2022 Report to Congress

Homeland Security

Science and Technology Directorate

Message from the Senior Official Performing the Duties of the Under Secretary of the Science and Technology Directorate

April 25, 2022

I am pleased to present the spend plan, "Critical Infrastructure Security and Resilience Research, Development, Test, and Evaluation," which has been prepared by the Science and Technology Directorate (S&T).

This document has been compiled pursuant to a requirement in the Infrastructure Investment and Jobs Act (P.L. 117-58, Division J). The spend plan includes a strategic framework.

Pursuant to congressional requirements, S&T is providing this report to the following Members of Congress:

The Honorable Lucille Roybal-Allard
Chairwoman, House Appropriations Subcommittee on Homeland Security

The Honorable Chuck Fleischmann
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Chris Murphy
Chair, Senate Appropriations Subcommittee on Homeland Security

The Honorable Shelley Moore Capito
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries about this report may be directed to Office of Legislative Affairs at 202-447-5890.

Sincerely,

Kathryn Coulter Mitchell

Kathryn Coulter Mitchell
Senior Official Performing the Duties of Under Secretary
for Science and Technology

Executive Summary

Critical Infrastructure Protection is vital to national economic security, and to national public health and safety.

S&T focuses on providing the tools, technologies, and knowledge products for the Nation's Homeland Security Enterprise as the research, development, test, and evaluation (RDT&E) arm of the Department of Homeland Security (DHS). S&T's aim, through the advancement of science and technology, is to strengthen and maintain secure, functioning, and resilient critical infrastructure.

S&T developed this strategic framework and spend plan for supporting critical infrastructure security and resilience, as required by the Infrastructure Investment and Jobs Act, working closely with DHS operational component partners. The strategic framework presented here provides the foundation for addressing key critical infrastructure security and resilience across the RDT&E lifecycle.

With this plan, S&T is taking a whole-of-government approach to connect strongly to and address critical infrastructure community needs. Executing this plan in the upcoming years will advance DHS's vision to enhance its capability to safeguard the American people, our homeland, and our values.

Critical Infrastructure Security and Resilience Research, Development, Test, and Evaluation Spend Plan

Table of Contents

I. Legislative Language

The Infrastructure Investment and Jobs Act (P.L. 117-58, Division J) states:

> For an additional amount for ''Research and Development'', $157,500,000, to remain available until September 30, 2026, for critical infrastructure security and resilience research, development, test, and evaluation: *Provided*, That the funds made available under this heading in this Act may be used for—
>
> (1) special event risk assessments rating planning tools;
> (2) electromagnetic pulse and geo-magnetic disturbance resilience capabilities;
> (3) positioning, navigation, and timing capabilities;
> (4) public safety and violence prevention to evaluate soft target security, including countering improvised explosive device events and protection of U.S. critical infrastructure; and
> (5) research supporting security testing capabilities relating to telecommunications equipment, industrial control systems, and open source software:
>
> *Provided further*, That not later than 90 days after the date of enactment of this Act, the Department shall submit to the House and Senate Committees on Appropriations a detailed spend plan for the amount made available under this heading in this Act…

II. Background

On November 15, 2021, President Biden signed the Infrastructure Investment and Jobs Act (P.L. 117-58, Division J), which assigned specific funding to the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) to conduct critical infrastructure security and resilience research, and development, test, and evaluation in the following areas:

(1) special event risk assessments rating planning tools;
(2) electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) resilience capabilities;
(3) positioning, navigation, and timing capabilities;
(4) public safety and violence prevention to evaluate soft target security, including countering improvised explosive device (IED) events and protection of U.S. critical infrastructure; and
(5) research supporting security testing capabilities relating to telecommunications equipment, industrial control systems (ICS), and open-source software.

This document provides S&T's strategic framework and spend plan implementing the Act.

III. Critical Infrastructure Security and Resilience Strategic Framework

This section structures the framework by focus area as follows:

- The **Strategic Context** provides background for why the focus area is important for critical infrastructure resilience;
- The **Goal** provides the overarching outcome or end state that S&T wants to achieve; and
- The **Technical Objectives** state what scientific or engineering accomplishments S&T will work toward.

Focus Area 1: Special Event Assessment Rating (SEAR) Planning Tools

Strategic Context

SEARs are applied to events that are not designated as national special security events. These tend to be pre-planned domestic special events that have been submitted and assessed using the SEAR methodology. Most of these events are state and local events that may require support augmentation from the Federal Government. The SEAR methodology was created by the DHS interagency special events working group to measure the risk of a terrorist attack at a special event. The SEAR methodology considers the threat, vulnerability, and consequences for each event and uses a mixed qualitative/quantitative analysis when assigning SEAR levels to special events submitted to DHS. The SEAR methodology determines the relative risk of each special event using a scenario-based assessment, using a variety of terrorist attack scenarios for each event to help determine the event's risk. Currently, there are 10 attack scenarios that are used as benchmarks for threats of concern to special events. The scenarios are limited to terrorism threats and are widely applicable to most special events. The SEAR methodology also considers the vulnerability and consequences for each event. SEAR levels are dynamic and may change from year to year because of changes in the event information or updates to the SEAR methodology.

Focus Area Goal

Ensure effective physical security at SEAR events. This includes enhancing the SEAR methodology and improving the dissemination of SEAR information.

Technical Objectives

1. Conduct a thorough review of the SEAR methodology and explore new methods, concepts, and modeling techniques to improve the SEARs and to enhance operational planning.
2. Perform a data needs and technology assessment for SEAR risk and event planning tools, considering the current and future threat landscape and advances in new technology and data.

3. Develop SEAR events protection portal containing security decision support tools for use by the Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security Division and regional Protective Security Advisors.
4. Test and demonstrate the new SEAR planning tools with stakeholders and produce new training resources.

Focus Area 2: Electromagnetic Pulse and Geomagnetic Disturbance Resilience Capabilities

Strategic Context

EMP and GMD events have the potential to disrupt or permanently damage electrical components and systems within the critical infrastructure sectors (e.g., ICSs, large power transformers, network routers, traffic controllers, and radio receivers/transmitters) and large-scale infrastructure (e.g., the electric power grid, communication networks, satellite networks, and interstate pipelines). Over recent years, several conclusions have been drawn as to the impacts of an EMP/GMD event on critical infrastructure based on research and modeling efforts. However, there is significant variability in the results, which happens for several reasons, such as understanding of the threat and threat environment; modeling assumptions; lack of relevant test data; and limited understanding of critical infrastructure components and their true vulnerabilities because of lack of testing. The variability in results makes it challenging to identify specific impacts confidently and to recommend actions and mitigations that should be taken to protect critical infrastructure from this threat. Additionally, although EMP hardening standards exist for military applications, they are often prohibitively expensive and impractical for private-sector critical infrastructure owners and operators to implement. Hence, the private sector has taken very little action taken to address this threat, which has the potential to affect the Nation at large.

This issue has been known for some time, and the recent Executive Order (EO) 13865, *Coordinating National Resilience to Electromagnetic Pulses,* and the 2020 National Defense Authorization Act directed specific efforts to understand better this threat, the risk that it poses, and its impacts on critical infrastructure. CISA, as the Sector Risk Management Agency for the Communications sector, is prioritizing building its knowledge and expanding its understanding of the impacts and effects of EMP/GMD events on the Communications sector.

The primary issue to address, from a DHS perspective, is the risk associated with the high-altitude EMP (HEMP) E1 effects on system electronics, particularly in the communications and information technology sectors. Other risks, namely HEMP E3 and GMD, are primarily threats to the electrical grid and are largely under the purview of the Department of Energy (DOE). Additionally, modeling the impact of an EMP event to a high level of fidelity is a challenging and expensive endeavor better suited for agencies such as the Defense Threat Reduction Agency or the DOE National Labs. DHS aims to leverage partner agencies' investments to inform its risk picture, which will drive the desired actions, mitigations, and protections within the private sector.

The existing concept for protecting critical infrastructure from EMP, as indicated by the EMP EO 13865, is to:

1. Identify what is critical;

2. Determine what critical systems, networks, and assets are vulnerable to EMP;
3. Determine if the vulnerability creates significant risk; and, if so,
4. Support industry in mitigating the risk.

A critical infrastructure system, network, or asset could be made resilient to the effects of HEMP E1. DHS has demonstrated this by incorporating EMP hardening measures into the modernized Federal Emergency Management Agency (FEMA) Primary Entry Point stations. The challenge, however, is the feasibility of incorporating these mitigations into private-sector systems and assets. Critical infrastructure owners and operators need additional information, knowledge, and guidance from the government to take relevant and pragmatic actions to mitigate the risk. For DHS to be able to provide this information, additional research is needed to help identify, target, and test the most vulnerable systems; to advise on reasonable mitigation techniques and methods; and to explore new concepts and design practices for protection that minimize the potential for energy coupling within a given system.

Focus Area Goal

Improve S&T's understanding of the effects of EMP/GMD events on communications infrastructure (and other critical infrastructure) and drive research activities to provide practical, data-driven, specific, and actionable information, concepts, techniques, technologies, and tools to critical infrastructure owners and operators to implement to protect their current and future communication systems from the impacts of an EMP event.

Guiding principles:

1. Information should include test results, best practices, and concepts of operation.
2. Tools should include models, commercially available and viable (tested and evaluated) mitigation solutions.
3. Rely on and leverage inputs and partnerships with critical infrastructure owners and operators as much as and whenever possible.
4. Make as much information as "shareable" as possible to include any models developed by this effort.

Technical Objectives

For any critical infrastructure system, component, subcomponent, or element, the following technical objectives are required to produce and deliver effective results. These objectives are derived from the requirements in the National Science and Technology Council report, *Research and Development Needs for Improving Resilience to Electromagnetic Pulses.*

1. Explore new or dual-use concepts for inherently minimizing energy coupling within a system or limiting exposure to the E-field.

2. Conduct a full set of modeling and validation testing of EMP impacts on critical infrastructure systems to identify critical vulnerabilities.

3. For identified critical vulnerabilities, determine and validate viable protection methods, technologies, and techniques through modeling and testing.

4. Develop industry-appropriate new EMP/GMD protection standards. The existing military EMP standard (MIL-STD-488-125) is more than two decades old and is not appropriate for critical infrastructure applications.
5. Package, share, and distribute information to include:
   - Models, tools, and test results.
   - Protection methods, concepts, technologies, and techniques, into best practices for industry use.
   - Workshops and industry days to facilitate information sharing.

Focus Area 3: Position, Navigation, Timing (PNT) Capabilities

Strategic Context

Per the 2013 National Risk Estimate, 13 of 16 critical infrastructure sectors are reliant on PNT services. Current PNT services are easily corrupted or disrupted. On February 12, 2020, President Trump signed an EO to strengthen the resiliency of U.S. critical infrastructure through responsible use of PNT. Many systems within U.S. critical infrastructure are designed with the assumption that PNT services (derived from the Global Positioning System (GPS)) will be available and are always correct. Because of this design, disruption or corruption of PNT service can cause safety-of-life issues or complete system failure in major systems such as wireless communications.

In 2016, the DHS PNT Executive Steering Committee was established to coordinate component activities on PNT resilience in response to a known GPS threat. DHS has made significant progress toward that goal, but the landscape also has changed rapidly since then. Other global navigation satellite systems (GNSS) have become operational and user equipment no longer uses just GPS but are designed as multi-GNSS systems. Additionally, there is a rapid emergence of new non-GNSS PNT services. These new services and systems contribute to a more resilient PNT landscape through source diversity and have their own limitations and vulnerabilities. Each new PNT source and the integration of these sources have hardware and software connections that expand the cybersecurity target set even further, creating a more robust and resilient system, but also increasing the potential for exploitation of undiscovered weaknesses. New capabilities also are giving rise to new technologies with greater reliance on PNT capabilities, including 5G and automation. This challenge is further complicated by the evolving risks of widespread, long-term GPS outages.

The current problem space consists of (1) the need to design and operate systems securely in an emerging landscape of a multi-PNT ecosystem with a larger set of attack surfaces; (2) future technologies having increasing dependence on PNT and the need to ensure that these are designed resiliently; and (3) mitigating an expanded range of PNT threats from localized, short-term interference to widespread, long-lasting disruptions.

Focus Area Goal

U.S. critical infrastructure and DHS missions must be resilient to PNT threats and disruptions, even in an evolving landscape where the multi-PNT ecosystem attack surfaces are larger, the incorporation of PNT dependencies into future technologies become greater, and the scale of impacts extends in range from localized, short-term interference to potentially widespread, long-lasting disruptions.

Solving these challenges will require DHS to work closely with industry as its adoption and deployment of solutions will be necessary to ensure critical infrastructure resilience. Therefore, DHS must not only work with industry to understand fully the impacts of these new threats, but to develop actionable tools, resources, and frameworks with industry adoption and deployment in mind.

Technical Objectives

1. Understand, validate, and characterize how current and future critical infrastructure operations and DHS missions degrade and fail in response to progressively challenging PNT disruption threat scenarios.
2. Develop standard frameworks and assessment processes for PNT service providers to evaluate the security and resilience of their services, including the signal structure and associated infrastructure elements (such as control and transmission segments).
3. Develop, demonstrate, and encourage adoption of concepts that will enable end-user systems to eliminate or limit the dependence on external PNT services.
4. Assess the PNT dependence of future and emerging technologies (e.g., 5G, unmanned aircraft system, automation) and identify measures to ensure their resilience to PNT disruption and manipulation.
5. Conduct industry outreach activities and publish best practices, guidance documents, and resources and tools to enable industry advancement on PNT resilience.
6. Advance and understand the feasibility of widespread adoption of resilient multi-PNT ecosystems through the development of concepts, techniques, technologies, and/or interface standards for alternate PNT sources and integration platforms, and ensure that they are designed with security and resilience.

Focus Area 4: Public Safety and Violence Prevention/Soft Target Security

Strategic Context

Soft Targets and Crowded Places (ST-CP), such as sports venues, shopping venues, schools, and transportation systems, are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack. Weapons used in ST-CP attacks range from the use of homemade explosives in IEDs and readily available weapons to a motor vehicle used in a ramming attack.

There are many types of threat actors who could attempt to target ST-CP and who share a common purpose—to harm Americans by violence. They include foreign terrorist organizations; "foreign fighters" (i.e., Americans and other Westerners who travel to conflict zones, learn bombmaking and other combat skills, and return to the U.S. to conduct attacks or to facilitate the spread of tactics and techniques in their communities); and other threat actors, such as domestic criminals and lone actors. The Intelligence Community has assessed that, for the foreseeable future, ST-CP will continue to remain attractive targets for various threat actors. An understanding of how the public reacts during these types of events would aid in the development of specific training to increase the survivability of such an attack, and in new policies and guidance for government leaders and first responders to be prepared better in their planning and response to these events.

Bad actors' tactics are evolving through observation of actual or perceived successes in the United States and elsewhere, trial and error, and the exchange of information over the internet and social media. Extremist literature provides the know-how through simple and clear instructions for making IEDs, and for using guns, knives, vehicles, and other readily accessible tools to kill and maim unsuspecting individuals. The fact that highly lethal attacks on ST-CP can be executed with little planning or expertise paired with the sheer volume of ST-CP presents a significant security challenge. The leveraging of software, data analytics, and machine learning could aid in the identification of these bad actors—traveling to and across the U.S., communicating with other members of their cell, and purchasing material items, (i.e., explosive precursor materials for the manufacturing of explosives)—and could aid in the disruption of a terrorist plot.

To provide enhanced security measures for ST-CP, DHS needs to understand better the current security readiness of ST-CP. The development of a standard methodology to assess the current level of readiness and security requirements is necessary to ensure consistent data for analysis. Using analytical modeling to identify the current level of security readiness, DHS will be able to develop specific training and best practices aimed to increase the security posture against identified threats. An additional output from this ST-CP security assessment will be previously unknown security requirements (i.e., healthcare and public health sector) that can be submitted into the RDT&E process.

Focus Area Goal

Enhance ST-CP security across the spectrum of prevention, protection, response, and mitigation. This includes enhancing the base of knowledge in public safety and violence prevention to soft-target security, strengthening physical security through capability advancements, and countering IEDs.

Technical Objectives

Public Safety and Violence Prevention to evaluate ST-CP security:

1. Conduct research to understand fully and support how human behavior affects positive safety and security outcomes in various threat scenarios, specifically countering IED events and other threat scenarios facing the infrastructure security community.
2. Examine public safety violence prevention research into terrorism, targeted violence, and mis/dis/mal-information for ST-CP.
3. Develop a standardized approach to risk assessment for hardening ST-CP.
4. Develop a data infrastructure that would allow CISA to code and input existing and future data better across threat scenarios, including IEDs.
5. Analyze and model trends and provide guidelines to deliver targeted trainings to specific audiences within the critical infrastructure community.

6. Conduct stakeholder outreach activities and publish resource guides and training materials to aid operational partners to advance ST-CP security.

ST-CP physical security and protection of U.S. critical infrastructure:

1. Conduct a thorough evaluation of soft-target security including examination of relative risks and trade-offs from soft-target hardening.
2. Investigate and develop capabilities that can be commercialized to enhance security against threat scenarios such as vehicle ramming threat and countering IEDs, with particular emphasis on special events.
3. Conduct stakeholder outreach activities and publish resource guides and training materials to aid operational partners to advance ST-CP security.

Focus Area 5: Security Testing Capabilities for Telecommunications Equipment, ICSs, and Open-Source Software

Strategic Context

Telecommunications: Today, telecommunications include much more than voice communications. Critical infrastructure owners, first responders, and DHS Component end-users rely on telecommunications networks to deliver data, text, images, video, and other critical information to achieve their mission. The networks used for these types of communication have security vulnerabilities that only increase with the continued growth of internet protocol-based technologies. Standards-based, secure, and interoperable telecommunication solutions are vital to mission success. The promotion of reliable, tested, standards-based encryption standards, such as Advanced Encryption Standard-256, will help to ensure a more resilient Homeland Security Enterprise. In addition to technology solutions, knowledge products including testing frameworks are needed to enable critical infrastructure owners, first responders, and DHS Component end-users to make informed procurement decisions to ensure security and interoperability.

Industrial Control Systems: ICS security is a growing concern. ICSs are at the heart of most critical infrastructure, enabling the control and management functions of critical infrastructure such as factories, power plants, water systems, ports, and other industrial facilities. These systems are vulnerable to cyberattacks, as demonstrated by recent real-world events. In addition, the number of internet-connected devices—the Internet of Things (IoT)—is forecasted to triple to more than 45 billion devices by 2030, enabling new applications in sectors as diverse as smart cities, smart homes, connected cars, e-health, etc. As adoption of these devices increases, the threat surface of the Nation’s critical infrastructure and key resources and their ICSs will expand dramatically. Proactive research is needed to inform best practices and standards on how to securely integrate these new edge devices into legacy ICSs while minimizing the risk of additional attack surfaces.

Open-Source Software: Open-source software refers to software that is open to read, edit, and use, usually as part of a larger software package being developed. This type of software has been gaining greater adoption as companies, individuals, and governments use and maintain these codes. The software is assumed to be "secure" because it is open for public scrutiny, edits, and contributions. Unfortunately, not all codes are scrutinized for security concerns, nor are all developers.

Focus Area Goals

Telecommunications: Enhance the interoperability and integrity, reliability, and security of critical communication systems for DHS Components through the promotion and use of standards-based solutions.

Industrial Control Systems: Leverage advanced methods and capabilities to inform the cybersecurity of legacy and bleeding-edge ICS from network-based cyber-attacks; get ahead of new potential cybersecurity challenges posed by the integration of IoT devices with ICS; gain a deeper understanding of the cross-sector and cross-organization dependencies and cascading effects of interconnected ICS.

Open-Source Software: Develop tools and capabilities that will enable innovation and make for a more informed, resilient end-user community that is able to mitigate security vulnerabilities and operational risk during the use of open-source software. Specific tools and capabilities may include the development of low-cost open-source software, recommended security guidance, and proposed governance as well as the development of training, testing frameworks, or studies/activities. A preliminary use case will include guidance and open-source software reference implementation to enable the development of innovative, open-source, standards-based, privacy-preserving, digital identity for secure implementation of digital identity information to ensure the integrity of credentialing activities across multiple domains.

Technical Objectives

Telecommunications:

1. Develop testing frameworks to ensure standardization and interoperability to mitigate operational and security risks.
2. Test and validate the integrity, availability, interoperability, and reliability of critical communication systems (first responders – land mobile radio, broadband, 5G) while supporting cross-government entities (e.g., Emergency Communications Cybersecurity Center).
3. Enhance resiliency for mobile network infrastructure through security research and testing with public/private partnerships.

Industrial Control Systems:

1. Research and develop new, advanced methods for increasing the security of legacy ICS targeting access and identity while leveraging concepts such as zero-trust architectures, and capabilities such as artificial intelligence/machine learning.
2. Conduct research to baseline security requirements for IoT devices with ICSs resulting in hardware/software standards and best practices.

3. Conduct development, testing, and evaluation to understand cross-sector and cross-organization dependencies and cascading effects, including physical consequences of interconnected ICSs.

Open-Source Software:

1. Secure current and future software development efforts from malicious attacks stemming from open-source software.
2. Nurture the development of open-source, standards-based, privacy-preserving, digital identity infrastructure for use by state and local governments, the Federal Government, and the private sector.

IV. Detailed Spend Plan

S&T Project	Purpose	Funding ($)	Funds Obligation Timeline
Focus Area 1: Special Event Risk Assessments Rating Planning Tools			
Critical Infrastructure Security and Resilience Research (CISRR) - SEAR Tools	Ensure effective physical security at SEAR events. This includes enhancing the SEAR methodology and improving the dissemination of SEAR information.	$9,166,250	FY 2022-2025
Focus Area 2: Electromagnetic Pulse and Geomagnetic Disturbance Resilience Capabilities			
CISRR - EMP and GMD Resiliency	Improve our understanding of the effects of EMP/GMD events on communications infrastructure (and other critical infrastructure) and drive research activities to provide practical, data-driven, specific, and actionable information, concepts, techniques, technologies, and tools to critical infrastructure owners and operators to implement to protect their current and future communication systems from the impacts of an EMP event.	$22,750,000	FY 2022-2025
Focus Area 3: Position, Navigation, Timing Capabilities			
CISRR - PNT	U.S. critical infrastructure and DHS activities must be resilient to PNT threats and disruptions, even in an evolving landscape where the multi-PNT ecosystem attack surfaces are larger. DHS must work not only with industry to understand fully the impacts of these new threats, but DHS also must develop and make available actionable tools, resources, and frameworks with industry adoption and deployment in mind.	$26,400,000	FY 2022-2025

S&T Project	Purpose	Funding ($)	Funds Obligation Timeline
Focus Area 4: Public Safety and Violence Prevention/Soft Target Security			
CISRR - Soft Target Physical Security	Enhance ST-CP security across the spectrum of prevention, protection, response, and mitigation. This includes enhancing the base of knowledge in strengthening physical security through capability advancements and countering IEDs.	$34,950,000	FY 2022-2025
CISRR - Public Safety and Violence Prevention	Enhance ST-CP security across the spectrum of prevention, protection, response, and mitigation. This includes enhancing the base of knowledge in public safety and violence prevention to soft target security.	$14,100,000	FY 2022-2025
Focus Area 5: Security Testing Capabilities for Telecommunications Equipment, Industrial Control Systems, and Open-Source Software			
CISRR - Telecommunications	Enhance the interoperability and integrity, reliability, and security of critical communication systems for DHS Components through the promotion and use of standards-based solutions.	$14,350,000	FY 2022-2025
CISRR - ICS	Leverage advanced methods and capabilities to inform the cybersecurity of legacy and bleeding-edge ICS from network-based cyber-attacks; get ahead of new potential cybersecurity challenges posed by the integration of IoT devices with ICS; gain a deeper understanding of the cross-sector and cross-organization dependencies and cascading effects of interconnected ICS.	$19,100,000	FY 2022-2025
CISRR - Open-Source Software	Develop tools and capabilities that will enable innovation and make for a more informed, resilient, end-user community that is able to mitigate security vulnerabilities and operational risk during the use of open-source software.	$11,250,000	FY 2022-2025

S&T Project	Purpose	Funding ($)	Funds Obligation Timeline
All Focus Areas			
Small Business Research Innovation (SBIR)	Per Section 9f of the Small Business Act, 15 United States Code (U.S.C.) 638, "Except as provided in paragraph (2)(B), each Federal agency which has an extramural budget for research or research and development of more than $100,000,000 for the fiscal year 1992, or any fiscal year thereafter, shall expend with small business concerns— (I) not less than 3.2 percent of such budget in fiscal year 2017 and each fiscal year thereafter, specifically in connection with SBIR programs which meet the requirements of this section, policy directives, and regulations issued under this section.”	$5,040,000	FY 2023
	Subtotal	**$157,106,250**	

Transfer to the Office of Inspector General			
Other Salaries and Expenses	Per Section 501 of H.R. 3684, one-quarter of one percent of the amounts made available under each heading in this title in this Act in each of fiscal years 2022 through 2026 shall be transferred to the DHS Office of the Inspector General for oversight of funding provided to DHS in this title in this Act.	$393,750	FY 2023
	Total	**$157,500,000**	

V. Conclusion

To use funds from the Infrastructure Investment and Jobs Act (P.L. 117-58, Division J) efficiently to conduct RDT&E activities for DHS Components, DHS S&T has created the CISRR Program. The program will report to Congress on the progress of CISRR research and development activities. The Infrastructure Investment and Jobs Act provides funding to:

- Perform currently unfunded customer requirements;
- Collaborate across various S&T offices and departments to get benefits for multiple DHS Components; and,
- Conduct important research and development to produce transitional products such as software, prototypes, and knowledge products.

Building on this strategic framework and spend plan, the CISRR Program is developing a Program Management Plan and forming the S&T and DHS Component teams needed to perform the work. Once teams are formed, the CISRR Program will work with various managers to execute the work over the next 5 years. S&T plans to: develop new modeling techniques to improve risk assessments and operational planning; test and evaluate prototypes and software; conduct research in burgeoning technology; and conduct demonstrations with partners to test new technology. S&T RDT&E efforts will strengthen critical infrastructure security across multiple DHS Components such as CISA, Transportation Security Administration, U.S. Customs and Border Protection, United States Secret Service, DHS Operations, First Responders Group, and United States Coast Guard.

Appendix A: Bibliography

- U.S. Cyberspace Solarium Commission. (March 2020). *Final Report.*
- U.S. Department of Commerce. National Telecommunications and Information Administration. (2021). *National Strategy to Secure 5G Implementation Plan.* https://www.ntia.gov/5g-implementation-plan.
- U.S. Department of Homeland Security. Office of Operations Coordination. (n.d.). *Fact Sheet: What are Special Event Assessment Rating (SEAR) Events?* https://www.dhs.gov/publication/special-event-assessment-rating-sear-events-fact-sheet.
- U.S. Department of Homeland Security. Office of Operations Coordination. (July 4, 2019). *Special Event Assessment Rating Methodology: Background Information*.
- U.S. Department of Homeland Security. DHS Directive 111-01-001. (July 1, 2021). *Special Events Coordination Instruction*.
- U.S. Department of Homeland Security. Office of Operations Coordination. (November 2019). *Office of Operations Coordination.*
- U.S. Department of Homeland Security. Cybersecurity and Infrastructure Security Agency, Office of Emergency Communications. (2018). *2018 SAFECOM Nationwide Survey Results: National-Level Summary.* https://www.cisa.gov/sites/default/files/publications/SNS%20Results_FINAL_508Compliant_02112021.pdf.
- U.S. Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. (2019). *National Emergency Communications Plan.* https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_1_0.pdf.
- U.S. Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. (2020). *CISA 5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation.* https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.
- U.S. Department of Homeland Security. (August 2019). *Positioning, Navigation, & Timing Strategy, 2019 – 2024.*
- U.S. Department of Transportation; U.S. Department of Homeland Security; U.S. Department of Defense. (2019). *2019 Federal Radionavigation Plan.* DOT-VNTSC-OST-R-15-01 https://www.navcen.uscg.gov/pdf/FederalRadioNavigationPlan2019.pdf.
- U.S. Government Accountability Office. (November 2021). Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector. https://www.gao.gov/assets/720/717685.pdf.
- U.S. National Science and Technology Council. Networking & Information Technology Research and Development Subcommittee and Machine Learning & Artificial Intelligence Subcommittee. (March 2020). *Artificial Intelligence and Cybersecurity: Opportunities and Challenges: Technical Workshop Summary Report*.

- U.S. National Science and Technology Council. Committee on Technology. Subcommittee on Future and Advanced Computing Ecosystem. (November 2020). *Pioneering the Future Advanced Computing Ecosystem: A Strategic Plan*.
- U.S. National Science and Technology Council. Committee on Science and Technology Enterprise. Networking & Information Technology Research and Development Subcommittee. Cyber Security & Information Assurance Interagency Working Group. (August 14, 2020). *FY 2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap.* Appendix to the Networking & Information Technology Research and Development Program: Supplement to the President's FY 2021 Budget.
- U.S. National Science and Technology Council. Committee on Science and Technology Enterprise. Networking & Information Technology Research and Development Subcommittee. (August 14, 2020). *The Networking & Information Technology Research and Development Program: Supplement to the President's FY 2021 Budget.*
- U.S. National Science and Technology Council. Committee on Science and Technology Enterprise, Subcommittee on Networking & Information Technology Research and Development and Committee on Technology, Subcommittee on Future and Advanced Computing Ecosystem. (October 2021). *National Strategic Computing Reserve: A Blueprint*.
- U.S. National Science and Technology Council. Committee on Homeland and National Security. Subcommittee on Resilience Science and Technology. Electromagnetic Pulse Research and Development Assessment Interagency Working Group. (June 2020). *Research and Development Needs for Improving Resilience to Electromagnetic Pulses.*
- U.S. National Science and Technology Council. Committee on Homeland and National Security. Subcommittee on Resilience Science and Technology. Positioning, Navigation, and Timing Research and Development Interagency Working Group. (August 2021). *National Research and Development Plan for Positioning, Navigation, And Timing Resilience*.
- U.S. White House. (February 26, 2013). Presidential Policy Directive 17. *Countering Improvised Explosive Devices*.
- U.S. White House. (March 26, 2019). Executive Order 13865. *Coordinating National Resilience to Electromagnetic Pulses.*
- U.S. White House. (February 12, 2020). Executive Order 13905. *Strengthening National Resilience Through Responsible Use of PNT Services.*
- U.S. White House. (January 15, 2021). Memorandum on Space Policy Directive 7. *The United States Space-Based Positioning, Navigation, and Timing Policy.*
- U.S. White House. (May 12, 2021). Executive Order 14028. *Improving the Nation's Cybersecurity.*

Appendix B: Authorities

- Title 6, United States Code (U.S.C.) § 182, "Responsibilities and authorities of the Under Secretary for Science and Technology." Title 6, U.S.C. § 188, "Conduct of research, development, demonstration, testing and evaluation."
- Title 6 U.S.C. § 112. Homeland Security Act of 2002 — All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A-119.
- Title 6, U.S.C. § 195f (a) - In general, In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and relevant owners and operators of critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of threats of EMP and GMD.
- Title 6, U.S.C. § 195f (d)(1)(C) – The Secretary of Homeland Security, in coordination with the heads of relevant Sector-Specific Agencies, shall – (i) without duplication of existing or ongoing efforts, conduct research and development to better understand and more effectively model the effects of EMPs and GMDs on critical infrastructure (which shall not include any system or infrastructure of the Department of Defense or any system or infrastructure of the Department of Energy associated with nuclear weapons activities); and (ii) develop technologies to enhance the resilience of and better protect critical infrastructure.
- Title 6 U.S.C. § 195f Section (d)(2)(A) – Report on the identification of technological options to improve the resilience of critical infrastructure to the effects of EMPs and GMDs and identifies gaps in available technologies and opportunities for technological. developments to inform R&D activities to Congress every 4 years following until 2032.
- Title 6 U.S.C. § 195f Section (d)(2)(B) – Identification of gaps in EMP/GMD knowledge base by reviewing existing test data and identifying any gaps in the test data.
- Title 6, U.S.C. § 194, "Enhancement of public safety communications interoperability."
- Title 6, U.S.C. § 195, "Office for Interoperability and Compatibility."
- Title 6, U.S.C. § 195a, "Emergency communications interoperability research and development."
- Title 6, U.S.C. § 571, "Office of Emergency Communications."
- DHS Delegation 10001 Revision 01, "Delegation to the Under Secretary for Science and Technology."
- DHS Directive 078-04, "Standards Policy Governance and Coordination"

Appendix C: Abbreviations

Abbreviation	Definition
CISA	Cybersecurity and Infrastructure Security Agency
CISRR	Critical Infrastructure Security and Resilience Research
DHS	Department of Homeland Security
DOE	Department of Energy
EMP	Electromagnetic Pulse
EO	Executive Order
GMD	Geomagnetic Disturbance
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HEMP	High-Altitude Electromagnetic Pulse
ICS	Industrial Control System
IED	Improvised Explosive Device
IoT	Internet of Things
PNT	Position, Navigation, Timing
RDT&E	Research, Development, Test, and Evaluation
S&T	DHS Science and Technology Directorate
SBIR	Small Business Innovation Research
SEAR	Special Event Assessment Rating
ST-CP	Soft Targets and Crowded Places
U.S.C.	United States Code