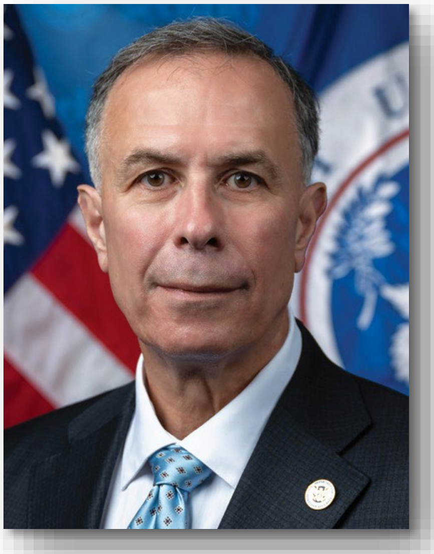
DHS Innovation, Research & Development Strategic Plan

Fiscal Years 2024-2030

Homeland Security

MAY 2024

LETTER FROM THE UNDER SECRETARY OF SCIENCE AND TECHNOLOGY



As the U.S. Department of Homeland Security (DHS) enters our third decade, the homeland security threat and hazard landscapes continue to evolve. Those who wish to do the Nation harm exploit the same technologies and pathways that enable American prosperity and our way of life. The frequency and impact of natural disasters increasingly challenge our resiliency. And innovations, such as the rapid development and wide adoption of Artificial Intelligence, are major disruptors of the homeland security enterprise (HSE) and empower our adversaries.

Innovation, Research and Development (IRD) initiatives provide DHS the key mechanisms to keep pace with this changing strategic environment. The technologies that emerge from our IRD investments are critical to ensuring our front-line operators have the tools they need to stay ahead of our adversaries and better prepare for and respond to natural hazards.

To ensure DHS has a strategic and integrated approach to IRD, I am proud to introduce the Department's Innovation, Research and Development Strategic Plan for Fiscal Years 2024-2030. This first-of-its-kind Strategic Plan identifies ways to coordinate IRD investments to maximize impacts across our components and missions. Carefully built through data collection and analysis, and crafted with stakeholders from across the Department, the Plan brings focus to our IRD portfolios by highlighting eight key, cross-cutting Strategic Priority Research Areas (SPRAs) that the Department will foster over the next seven fiscal years.

In addition to ensuring that the Plan informs DHS's resource decisions, we will work closely with our key HSE partners, Congress, industry, academia, and other stakeholders to catalyze the Plan's IRD priorities. Together, we will continue to build the vital capabilities needed to secure the Homeland.

Sincerely,

Dr. Dimitri Kusnezov

Under Secretary for Science and Technology

TABLE OF CONTENTS

EXECUTIVE SUMMARY

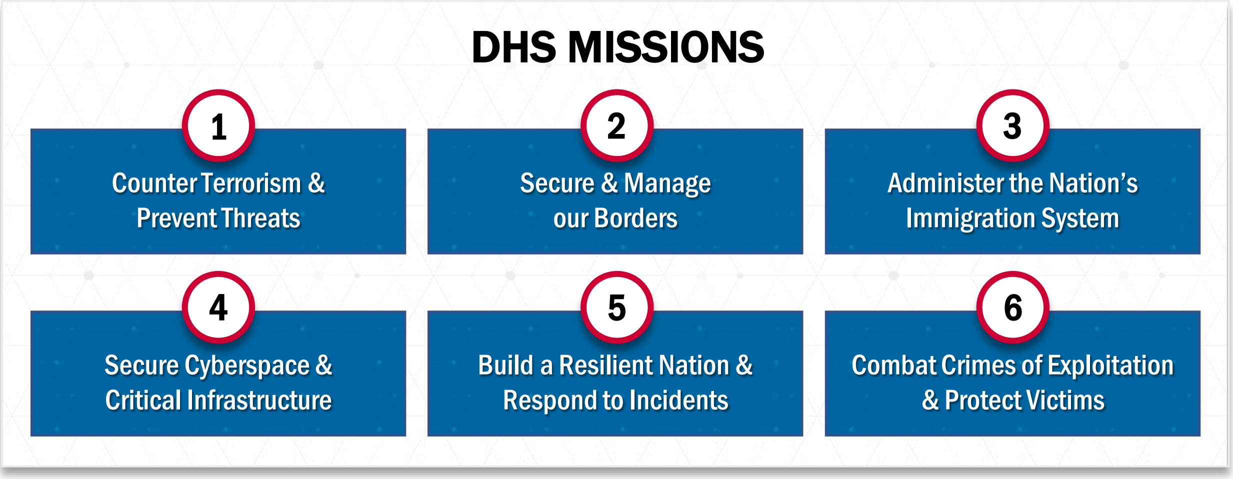
The Secretary seeks to ensure technological improvement efforts, both across the Department of Homeland Security (DHS) and with external partners, are coordinated and integrated to achieve optimal outcomes for its operators and other stakeholders. Innovation, research and development (IRD) efforts provide the primary means to realize this objective. IRD helps build the capabilities needed to address the homeland security threats and hazards of today and tomorrow.

These threats and hazards to the United States (U.S.) homeland have grown considerably more diverse and complex over the past two decades of DHS's existence. Cyberattacks, the opioid and synthetic drug crisis driven by transnational criminal organizations (TCOs), the proliferation of health security biothreats, and domestic violent extremism (DVE) are but a few of the threats increasingly endangering communities and individuals across the country. As climate change triggers increasingly severe and frequent disasters, such as hurricanes, drought, wildfires, and extreme heat, the Department requires enhanced preparedness and response capabilities to deal with these and other natural hazards.

Technology is a powerful force multiplier, improving efficiency and effectiveness to meet these and the many other challenges facing the Department and the wider homeland security enterprise (HSE). Emerging technologies not only provide opportunities for DHS to enhance response capabilities, but also pose potential future threats from those that wish to exploit them to harm our way of life. A critical goal of the IRD community is to utilize state-of-the art capabilities to protect and defend the homeland from these myriad risks.

To optimize DHS-wide IRD, the Department formalized the first of its kind Innovation, Research, and Development Coordination (IRDC) Council, co-chaired by the Under Secretary of Science and Technology and the Under Secretary of Management and comprising Senior Executive Service representatives from across all DHS Components. This Council serves as the senior-level executive body overseeing DHS-wide coordination, strategic planning, and long-term resourcing of IRD, which includes basic research, applied research, development, testing and evaluation; technology improvement; and innovation efforts. This Council is charged with improving synchronization of technology improvement efforts across the enterprise; enhancing information sharing across IRD and acquisition stakeholders; and increasing transparency, traceability, unity of effort, and value to DHS-wide IRD activities. This body is also chartered to inform resource decisions and develop strategies, beginning with this document, to strengthen IRD investments throughout DHS.

The DHS IRD community spans the Department and includes all IRD investments made to support HSE missions. This Strategic Plan utilizes information collected in Fiscal Year (FY) 2023, including IRD current state initiatives, emerging technologies analyses, and individual operational Component future trends assessments. The Plan also assesses trends across future capabilities and points to opportunities for the Department to utilize IRD in a cross-cutting manner to advance the DHS Missions and Objectives identified in the third *Quadrennial Homeland Security Review* (2023).



DHS MISSIONS

1 Counter Terrorism & Prevent Threats

2 Secure & Manage our Borders

3 Administer the Nation's Immigration System

4 Secure Cyberspace & Critical Infrastructure

5 Build a Resilient Nation & Respond to Incidents

6 Combat Crimes of Exploitation & Protect Victims

Using this philosophy, the Department has adopted the concept of a Strategic Priority Research Area (SPRA), a cross-cutting assembly of enduring scientific efforts which provides a means for addressing priority needs across multiple HSE mission areas. DHS has identified eight (8) SPRAs which will improve internal DHS collaboration, guide the resource allocation plan (RAP) development as part of the planning, programming, budgeting, and execution (PPBE) cycle for FY 2026-2030 and, as applicable, subsequent RAP cycles, and serve as a demand signal to industry, interagency, academic, and international communities on future partnerships and collaborations.

Strategic Priority Research Areas	*DHS Mission Alignment*					
	1	2	3	4	5	6
Advanced Sensing	✓	✓	✓	✓	✓	
Artificial Intelligence and Autonomous Systems	✓	✓	✓	✓	✓	✓
Biotechnology	✓	✓	✓	✓	✓	
Climate Change	✓	✓	✓	✓	✓	
Communications and Networking	✓	✓	✓	✓	✓	✓
Cybersecurity	✓	✓	✓	✓	✓	✓
Data Integration, Analytics, Modeling and Simulation	✓	✓	✓	✓	✓	✓
Digital Identity and Trust	✓	✓	✓	✓	✓	✓

INTRODUCTION

Vision

By Fiscal Year 2030, DHS reduces the nation's risk from homeland security threats and hazards through optimized innovation, research, and development investments that improve the efficiency and effectiveness of its missions.

Background

Protecting our nation requires timely responses to rapidly evolving dangers while protecting against longer-term homeland security threats and hazards. To meet these complex operational needs, innovation, research and development (IRD) initiatives and investments are critical to ensure the Department of Homeland Security (DHS) has the tools to help secure our nation. Given limited resources, the Department must identify and prioritize cross-cutting solutions that can be successfully applied in multiple, diverse operational environments.

While historically DHS has supported research and development (R&D), investments in innovation are newer and growing in scope and number across all DHS Components, whether through technological improvements or process efficiencies. The combination of these innovation and R&D investments will benefit from increased awareness and coordination. The Secretary's Calendar Year (CY) 2023 priorities captured this, seeking to "ensure R&D across the Department and with external partners are coordinated and integrated."

To accomplish this goal, this coordinated DHS IRD Strategic Plan focuses on current efforts and longer-term Departmental investments. The Plan also highlights complementary efforts underway across the HSE, consisting of federal, state, local, tribal, territorial, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of the United States and its people. The Plan inventories current and future IRD efforts within DHS, organized by the DHS Missions and Objectives as articulated in the third *Quadrennial Homeland Security Review* (2023). By capturing these initiatives in a comprehensive plan, the Department can identify cross-cutting IRD themes that provide opportunities for making impacts towards meeting multiple desired outcomes. These are articulated as Strategic Priority Research Areas (SPRAs), cross-cutting assemblies of enduring scientific efforts which provide a means for addressing priority needs across multiple HSE mission areas and provide the Department an overarching path for future investments to guide the RAP development as part of the PPBE cycle for FY 2026-2030 and, as applicable, subsequent RAP cycles.

Guiding Principles

The DHS IRD Strategic Plan is strongly influenced by and aligned with the following key documents:

- *Third Quadrennial Homeland Security Review*
- The *DHS Secretary's CY 2023 Priorities*
- DHS-wide IRD Projects Inventory - *DHS R&D Projects FY 2022 Report to Congress* in accordance with the *National Defense Authorization Act* (NDAA)
- *DHS Science and Technology Directorate (S&T) Technology Centers Research Agenda*
- *Office of Management and Budget (OMB) Circular A-11, "Preparation, Submission, and Execution of the Budget"*
- DHS Innovation, Research, and Development Coordination Implementation Guidance
- *DHS Resource Planning Guidance, Fiscal Years 2025-2029*
- *National Biodefense Strategy and Implementation Plan 2022*
- *National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture*
- *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*
- *The National Cybersecurity Strategy (2023)*

To protect the American people, DHS must uphold constitutional, statutory, regulatory, policy, and other requirements during the execution of programs and activities of the Department, including IRD efforts. The Department must ensure that the privacy, civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland. Therefore, within the context of IRD, the highest ethical standards must be employed to safeguard the dignity, rights, safety, and privacy of human subjects and other stakeholders. Additionally, the Department's IRD efforts must account for cultural and contextual factors that could influence findings and the use of those findings.

Strategic Plan Development

The strategic planning team took a collaborative, data-driven approach to develop this Plan, including establishing a DHS-wide Tiger Team; conducting and analyzing a series of data calls; and hosting a validation meeting and workshop with Component subject matter experts. Specific planning, data collection, and analysis activities included:

- Completed DHS-wide IRD projects data collection inventory in January 2023 that fed the *DHS R&D Projects FY 2022 Report to Congress* required by the FY17 *National Defense Authorization Act* (NDAA), P.L. 114-328;

- Established the IRD Strategic Plan Tiger Team and held meetings since November 2022;
- Conducted an IRD Strength, Weakness, Opportunity and Threat analysis and hosted Department-wide validation meetings in February 2023;
- Coordinated a DHS-wide Component future trends assessment data call in April 2023; and
- Held a two-day workshop in April 2023 with participation from planners and operators from across the Department to identify and validate desired capabilities and end states to inform future IRD development.

Partnerships and Implementation

The current IRD efforts captured in this Plan comprise a network of government and private sector entities across the globe, including industry, academia, Federally Funded Research and Development Centers (FFRDCs), other federal agencies, and international partners that work together to address a range of current and emerging threats and hazards. DHS will continue to conduct this vital work across the HSE and with public and private sector research partners while broadening partnerships with non-traditional entities to bring in novel approaches to support meeting operational challenges. This will be done while also ensuring that U.S. research, intellectual property, and technology is properly protected from theft and espionage. Through these partnerships, DHS will reduce risks from threats and hazards by enabling an expanded awareness of new technology developments and innovations that can be leveraged for the HSE mission areas.

DHS pursues an enterprise-wide approach to address IRD needs through basic research, applied research, development, test and evaluation, technology improvement, and innovation efforts providing solutions across missions. Depending on the desired outcome for the mission, associated challenges, and the existing science and technology base, these efforts provide material and non-material solutions. Within DHS, the IRDC Process is structured to improve the synchronization of IRD efforts across the enterprise; enhance information sharing across IRD and acquisition stakeholders; and increase transparency, traceability, unity of effort, and value to DHS-wide IRD activities. Coordinated by S&T and DHS Management, the IRDC Process is the mechanism by which this Plan will be executed, including the development of implementation plans for DHS-wide priorities that will guide the allocation of resources. Part of this includes assessments on the alignment of Department-wide IRD activities and needs with the IRD Strategic Plan to identify recommendations on the most impactful cross-Component opportunities to inform high priority needs. The IRDC Council will make decisions regarding how to best use DHS's resources to address high priority needs based on the outputs from these implementation activities, specifically guiding RAP development as part of the PPBE process.

INNOVATION, RESEARCH & DEVELOPMENT TO MEET DHS MISSIONS & OBJECTIVES

IRD initiatives and investments are critical to realizing success across DHS's Missions and Objectives. They should influence internal business processes, including budget development and acquisitions, as well as policy development and partner engagements. The following sections utilize the DHS Missions and Objectives identified in the third *Quadrennial Homeland Security Review* as a framework to identify enduring challenges as well as current and future IRD activities making impacts towards addressing those challenges.

DHS Mission One: Counter Terrorism and Prevent Threats

Mission One is achieved through collecting, analyzing, and sharing actionable intelligence and information; preventing and disrupting terrorist and nation-state threats; protecting leaders and designated individuals, facilities, and events; and identifying and countering emerging and chemical, biological, radiological, nuclear, and explosive (CBRNE) threats. For mission success, DHS makes IRD investments in solutions to counter all forms of domestic and international terrorism, as well as emerging threats arising from the malicious use of new technologies. In conducting IRD to meet these objectives, DHS explores the opportunities of utilizing emerging technologies as solutions to enhance capabilities, as well as address challenges associated with the nefarious use of these technologies as emerging threats for those seeking to do harm to the HSE.

The following section outlines challenges, relevant current IRD activities, and future capabilities for each Objective under this Mission.

Objective 1.1:
Collect, Analyze, and Share Actionable Intelligence and Information

Securing the homeland requires an understanding of the dynamic nature of current threats and awareness of the emergence of new threats, hazards, incidents, or events. In accordance with this Objective, DHS works to ensure that our Components, federal, state, local, tribal, and territorial (FSLTT) partners, and international collaborators have actionable information and intelligence. This intelligence and information support real-time situational and domain awareness. It also affords DHS and its partners the flexibility and knowledge required to anticipate changes to threat climates and prepare appropriate responses, such as the deployment of resources to high-risk locations. In addition, DHS Components require connected, purpose-built data systems and forensic tools, which enable enterprise-wide data sharing and a centralized data analytics platform to facilitate collaboration across DHS Components. Such systems and tools must safeguard the dignity, rights, safety, and privacy of human subjects, stakeholders, and other affected entities and participants.

Current IRD investments associated with this Objective include the establishment and enhancements of core information sharing architectures to enable DHS Headquarters elements and Components to meet mission critical information sharing, domain awareness, and multi-agency operational coordination needs. In addition, DHS is developing a platform to enable knowledge products and tools to be effectively shared with the wider HSE to promote communication, scientific understanding, and CBRNE risk awareness.

For mission success, future IRD initiatives through FY 2030 will require the continued development of capabilities for domain-agnostic information sharing across various classification levels and the ability to share information in real-time to enable the rapid mitigation of threats. This necessitates readily available and highly resilient critical communications, services, and information sharing capabilities for all DHS Components and various partners – including first responders – using emerging technologies and communications networks. International partnerships must be expanded to facilitate increased sharing of threat information. Finally, to ensure maximum efficacy of these advancements, collaborations must be fostered, and appropriate policy practices and agreements established, to protect the parties involved while creating mutually beneficial environments for coordination.

Objective 1.2:
Prevent and Disrupt Terrorist and Nation State Threats

In meeting this Objective, DHS must be united in its approach to preventing and disrupting threats from domestic and international terrorism, including DVE, homegrown violent extremists, nation state threats, targeted violence and terrorism, lone offenders, and small groups of individuals motivated to violence by a broad range of racial, ethnic, political, religious, anti-government, societal, or personal ideological beliefs or grievances. Policymakers and operational end users need to make informed decisions to identify and prevent action by potential offenders, mitigate vulnerabilities in critical infrastructure, and enhance community resilience.

DHS must also prevent foreign threat actors from exploiting travel, trade, and financial systems for illicit purposes. This requires deterring, detecting, and denying access to individuals who may pose a threat to the United States while also supporting individual privacy and redress opportunities to ensure that screening and vetting programs keep pace with evolving threats, technologies, and operational realities.

Current IRD investments under this Objective are being driven by the need to form strategic insights into the motivations and enabling actions behind human trafficking, violent extremism, insider threats, and terrorism. This is part of a wider effort to develop an analytical system to better understand threats, risk, and vulnerabilities to the homeland.

For mission success, future DHS IRD initiatives through FY 2030 must enable the Department to launch and reinforce a multi-layered prevention architecture to minimize threats as they evolve while enhancing emergency preparedness and response. Finally, multi-layered screening and vetting architectures and identity verification technologies must be enhanced to prevent terrorist travel.

Objective 1.3:
Protect Leaders and Designated Individuals, Facilities, and Events

For this Objective, DHS must ensure the safety and security of designated persons to include the nation's highest elected leaders and visiting foreign heads of state and government. DHS must also secure National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events and protected federal facilities. Soft targets – such as schools, sports venues, transportation facilities, shopping venues, and places of worship –must be secured without limiting traffic and while protecting privacy, civil rights, and civil liberties. The challenges that arise in the event of cascading and overlapping special events further complicate advancing this Objective.

Current IRD activities associated with this Objective are focused on developing technologies for detecting, deterring, mitigating, and responding to targeted violence and exploring the application of a layered and integrated capability to safely screen for potential threats to secure soft targets. Investments are being made into capabilities to ensure the safety, security, and/or protection of people, facilities, or assets to include countering threats posed by nefarious unmanned aircraft systems (UAS); enhanced detection for Weapons of Mass Destruction (WMD), improvised explosive devices, weapons, and other CBRNE materials, devices, or agents; explosives detection and mitigation, perimeter protection technologies, and hardening structures; persistent, inexpensive networked sensors; forensic video technologies; and enhanced security for hostile vehicle mitigation such as vehicle ramming.

For mission success, future DHS IRD initiatives through FY 2030 will require investing in technologies and approaches for a layered and integrated automated threat detection capability, allowing FSLTT and other security stakeholders to safely screen people and their belongings for potential threat materials and contraband. Additionally, these technologies and approaches must be suitable for use in soft target venues and crowded places (ST-CP), where people are generally in unstructured clusters, without impacting the speed of travel. This will require improving current security capabilities for screening people and their belongings, such as increasingly accurate biometric capabilities to improve identity validation and verification of people accessing secure Federal facilities or other sensitive sites while also safeguarding privacy. Also urgently required are new and improved capabilities for continuous wide-area WMD threat monitoring. DHS will also explore mechanisms for reducing burden on those providing protective services through process automation and effective training.

Objective 1.4:
Identify and Counter Emerging and Chemical, Biological, Radiological, and Nuclear Threats

Enhancing preparedness, response, mitigation, and resilience requires DHS to have awareness of, and ability to rapidly identify and be able to counter, WMD and other CBRNE and health security threats, including those to the DHS workforce, in accordance with this Objective. WMD and other CBRNE threats include the full spectrum of incidents caused by threat actors with the intent to do harm, as well as natural events and accidents involving CBRNE material. The Department works in concert with a wide range of FSLTT and private industry partners to identify and counter these security threats, which include all incidents with public health impacts or other effects on the food and agricultural industry, veterinary sector, and health and economic security of the United States. Health security threats may result from acts of terrorism, theft or illicit use of dangerous pathogens, accidental releases, or other hazards such as current and emerging infectious diseases.

Under this Objective, DHS maintains awareness of emerging technologies that can be leveraged by threat actors for nefarious deeds but also by DHS if used to improve our mission execution. Such technologies can include artificial intelligence (AI), quantum information science, advanced communications technologies, microelectronics, nanotechnology, high-performance computing, biotechnology and biomanufacturing, robotics, advanced manufacturing, financial technologies, undersea technologies, and space technologies.

DHS's IRD activities which support this Objective currently span the WMD, other CBRNE, health security, and emerging threats spaces. These activities include approaches to fill in critical knowledge gaps on chemical and biological threat agents such as through testing to gain a foundational understanding of what these threats are, better preparing the Department to detect and counter them, as well as advancing the materials and technologies used to detect radiological and nuclear threat objects. DHS is investing in the development of new or enhanced CBRNE detection technologies that address detection and identification gaps in fielded environmental monitoring and biological detection capabilities, with improved performance over existing capabilities through reduced false alarms and near real-time detection, and which are more robust and cost effective. DHS is exploring a variety of methods for environmental biological threat detection indoors and outdoors, to include agent-agnostic approaches, multiplexed detection, sensor redesigns for urban environments, microfluids-based biodetection, autonomous presumptive identification, modifications to extend assay shelf life in the field, and enhancements for biosurveillance to enable early warning, real-time monitoring, and timely detection.

In the area of chemical threat detection, there is a focus on detecting a broad span of chemical threats in a range of scenarios, including at low concentrations encountered after an exposure or release. DHS activities include advanced non-contact/stand-off and wide-area approaches, detecting shielded chemical threats, characterizing gas-generating reactions, and rapid screening approaches

For radiological and nuclear threat detection, high energy resolution, high sensitivity, and more robust detectors are being developed for small and large form factors such as radioisotope identification devices, spectroscopic personal radiation detectors, and Radiation Portal Monitors. Another major focus is on improving the ability to detect shielded materials by using active probes (e.g., x-rays and neutrons) to inspect cargo and vehicles for dense objects or unique signatures characteristic of shielded radioactive or nuclear materials. Enhanced linear accelerators and high sensitivity, more robust detectors are being investigated to significantly enhance detection of shielded Special Nuclear Material in conveyances.

Across the CBRNE threat detection space for this Objective, the Department is also exploring ways to utilize sensor data in conjunction with other contextual information, advanced data analytics, and artificial intelligence/machine learning (AI/ML) to monitor live data streams to detect anomalies, classify data types, such as images, pixels, or particle counts, and integrate data from multiple sources to create context-rich data sets for analysis. In the realm of health security threats, DHS is working with lead U.S. Government Departments and Agencies on IRD activities exploring the development of multi-pathogen detection countermeasures that will provide faster and more comprehensive identification to enhance protection by limiting the spread and size of an outbreak. DHS is pursuing rapid, pen-side diagnostic tools and other countermeasures for high priority transboundary animal diseases such as African Swine Fever, Foot-and-Mouth Disease, and Rift Valley Fever. Finally, DHS is investing in identifying emerging risks to the HSE, including adversarial use of emerging technologies, understanding how emerging technologies could positively or negatively impact future operations while simultaneously exploring the potential for emerging technologies to provide cutting-edge solutions to current and anticipated operational challenges in areas such as advancements in detection, communications, and navigation.

For mission success, future DHS IRD initiatives through FY 2030 must enable anticipation of threats as early as possible and provide rapid, real-time, high confidence, cost effective detection of WMD, other CBRNE, and health security threats. This requires employing new approaches, such as autonomous detection and tracking of threats while simultaneously monitoring or responding to multiple targets at once; the ability to detect biological threats through agent-agnostic detection; alternative, non-traditional WMD, other CBRNE, and health security detection signatures; multi-threat detection in a single platform; and advanced algorithms such as machine learning (ML) for enhanced operator decision making.

The root causes behind dynamics in the environment (e.g., changing weather patterns, supply chains) that can impact the prevalence of existing pathogens and pests or emergence of novel pathogens in the food, agricultural, and veterinary sectors must be better understood to enable DHS to predict and rapidly detect these threats. DHS must continue to work with interagency partners to accelerate the development of next-generation vaccines and other countermeasures such as depopulation, decontamination, and disposal methods to identify, respond to, and recover from food and agriculture sector impacts, including current and emerging foreign animal disease threats to livestock and pathogens or pests which can impact food and crops. These efforts must include ensuring that DHS's working animals are protected from the dangers of current and emerging animal diseases and other threats. Finally, the Department will continue to maintain awareness of and remain vigilant of emerging technologies to better position us to prepare for and respond to new potential threat vectors.

The root causes behind dynamics in the environment (e.g., changing weather patterns, supply chains) that can impact the prevalence of existing pathogens and pests or emergence of novel pathogens in the food, agricultural, and veterinary sectors must be better understood to enable DHS to predict and rapidly detect these threats. DHS must continue to work with interagency partners to accelerate the development of next-generation vaccines and other countermeasures such as depopulation, decontamination, and disposal methods to identify, respond to, and recover from food and agriculture sector impacts, including current and emerging foreign animal disease threats to livestock and pathogens or pests which can impact food and crops. These efforts must include ensuring that DHS's working animals are protected from the dangers of current and emerging animal diseases and other threats. Finally, the Department will continue to maintain awareness of and remain vigilant of emerging technologies to better position us to prepare for and respond to new potential threat vectors.

DHS Mission Two: Secure and Manage our Borders

Mission Two is achieved through securing and managing air, land, and maritime borders; facilitating lawful trade and travel; and countering TCOs and other illicit actors. To support the Objectives under this mission, the DHS IRD community invests in border security technologies and other solutions to prevent illicit movement and the illegal entry or exit of people, weapons, dangerous goods, and contraband. IRD also supports solutions that help manage risks surrounding people and goods in transit. The following section outlines challenges, relevant current IRD activities, and future IRD capabilities for each Objective under this Mission.

Objective 2.1:
Secure and Manage Air, Land, and Maritime Borders

For this Objective, DHS operational elements, law enforcement (LE), and first responders must maintain persistent air, land (surface and sub-surface), and maritime (surface and sub-surface) domain awareness to detect, identify, track, and classify anomalies and objects of interest; to deploy predictive capabilities; and to connect disparate events. Converging mission requirements, emerging asymmetric threats, evolving technologies, and critically strained resources require advanced technologies that produce efficient, force-multiplying domain coverage to improve operational efficiency and reduce the lifecycle costs of operational technologies.

Current IRD activities associated with this Objective are focusing on the detection, investigation, and forensic analysis of cross-border tunnels, monitoring along challenging pathways and between ports of entry for threats, in addition to the abilities to detect, track, identify, classify, and counter small manned and unmanned aerial systems, ground-based objects and humans, and small surface vessels utilizing land, air, maritime, and space-based platforms. Additional investments support autonomous power generation capabilities in remote locations for embedded sensors, as well as mobile surface and subsurface detection capabilities along the land borders and beyond-line-of-sight communications capabilities.

For mission success, future DHS IRD initiatives through FY 2030 will provide continuous improvements to the reliability, timeliness, accuracy, and autonomy of detection capabilities to provide persistent domain awareness and enhance the detection, tracking, identification, and classification of humans and objects of interest. Furthermore, the ability to automatically analyze, communicate, and share this information across stakeholder communities in all domains seamlessly is a force-multiplying factor that will help alleviate operator burden, provide enhanced situational awareness, better understand trends, and improve forecasting. In addition, predictive analytic capabilities to identify locations of potential illicit activity in between ports of entry by utilizing trends in illegal trade and smuggling routes, examining existing coverage capabilities, and considering vulnerable border environments will improve overall response and resource allocation decisions. All system capabilities will need to have software and network security provisions to prevent malicious cyber influences and maintain data integrity.

Objective 2.2:
Expedite Lawful Trade and Travel

To expedite and ensure the integrity of legitimate trade and travel in accordance with this Objective, DHS works to develop new operational concepts and technologies for improved supply chain security, strengthened traveler screening, and enhanced cargo screening. Such enhancements must not negatively impact U.S. economic prosperity. DHS must also be able to operate in remote maritime environments, including the Arctic, to conduct our trade and travel facilitation mission, as well as meet our enforcement and response commitments. Upgraded tools are also critical to conduct rapid and accurate port and waterway health assessments, analyze conditions of ports or waterways after incidents or disasters, and develop risk-based approaches for mitigation, response, and recovery.

Current IRD activities associated with this Objective focus on improvements to examination technologies and techniques for enforcement of counterfeit, unsafe, and fraudulent goods inspections, as well as fraudulent mail interdictions. These activities are crucial given the increasing volume and complexities of international trade and mail. Investments are also improving air cargo screening and imaging capabilities, in addition to data visualization and analytics capabilities to track cargo and people to improve port of entry (POE) automated targeting systems. Existing IRD activities are exploring improvements to mechanisms for non-intrusive inspection of cargo, people, baggage, and goods to enhance detection of threats with reduced false alarm rates, including explosives and chemicals, while making them faster, less invasive, and cost effective through automation and improved ML algorithms. DHS is investigating enhanced biometrics capabilities grounded in rigorous scientific study and analysis to improve identity validation and verification of individuals arriving or departing POEs on foot or within a vehicle. Other IRD investments include utilization of space-based platforms to enhance communications, intelligence, reconnaissance, and surveillance in remote maritime environments, including the Arctic, and data analytics to provide timely alerting to increase the ability to detect and respond to illicit maritime activities or emergency situations in a timely manner.

For mission success, future DHS IRD initiatives through FY 2030 will provide fully automated, non-intrusive, cyber-protected, reliable, and cost-effective scanning capabilities for cargo, people, baggage, and goods to allow for seamless flow of trade and travelers with minimal need for officer or agent involvement. This will reduce operator cognitive load, freeing resources to focus on higher priority duties. For example, the ability to have real-time walk-by sensing, credential authentication and fraudulent document detection, video analytics, and risk-based screening would both enhance security and improve an airport passenger's curb-to-gate experience. Airport scanning systems need the ability to automatically detect concealed explosive and chemical threat materials. Integrated, remote imaging analysis and authentication of people, baggage, and goods with international partners will further facilitate global trade and travel.

In addition, real-time communication infrastructure and capabilities will be required in remote maritime environments to effectively safeguard transportation systems, protect against illicit activity, and support operations during maritime hazards, such as icebergs and inclement weather (e.g., heavy fog). All information technology (IT) systems will require fully protected capabilities to protect from cyberattacks to ensure robust supply chain risk management, information sharing, policy/regulation development, and enforcement for the Marine Transportation System (MTS).

Objective 2.3: Counter Transnational Criminal Organizations and Other Illicit Actors

TCOs are operating globally, committing fraud, counterfeiting, and engaging in illicit smuggling and trafficking of persons, drugs, arms, currency, wildlife, and other natural resources. Sophisticated criminal networks can easily appear, disappear, and reorganize in response to opportunities and authority gaps. These networks function as complex social structures across the cyber and physical spaces, and operate at a variety of scales, ranging from local to international. While technological innovations promise continuing improvements in the quality of life for individuals around the globe, criminal organizations are capitalizing on these transformative advances to become more agile and expand their illicit activities. To counter TCOs and other illicit actors and meet the desired outcome for this Objective, DHS will explore adoption of a unified approach developed by connected, purpose-built data systems, analytical and forensic tools, and centralized data analysis systems that enable enterprise-wide data sharing and collaboration across Components.

Current IRD activities associated with this Objective include development of digital forensic tools and a central unified framework that encourages collaboration and provides digital media exploitation capabilities designed to automate and augment current manual processes to combat illicit activities, such as cybercrimes and money laundering. Investments support development of enterprise collaboration platforms to enable computer vision for object and activity detection, voice semantic analytics, natural language processing (NLP) of unstructured text documents, information fusion for entity resolution, automated data schema generation, and tagging to move into the classified environment. DHS is exploring development of analytics, such as deep learning algorithms for decision support, data visualization, and pattern recognition, to exploit available data (e.g., dark web commerce, cryptocurrency transactions), detect deepfake videos and synthetic voices, and fuse sensor information with other data to discover and disrupt TCO activities such as cybercrime and drug smuggling operations.

For mission success, future DHS IRD initiatives through FY 2030 will advance seamless integration of interagency and international intelligence sharing framework capabilities on TCO activities needed to target, identify, and dismantle criminal networks. Analytics efforts should be expanded to counter money laundering of specified unlawful activities beyond drug smuggling, including terror financing, financial fraud, human trafficking, human smuggling, import/export violations and sanctions violations. Automated digital media exploitation and forensic alerting of nefarious TCO cyber activity are needed to enhance the Department's ability to disrupt these threats. DHS must remain ahead of criminal actions, gang activities, and threats before they reach the homeland. This can be achieved through anticipatory mechanisms, such as robust predictive analytics and forecasting using cutting-edge methods, agent-based models, and game theory. These approaches require good use cases, training data, and continuous training for dealing with adaptive illicit behaviors. Finally, given its unique border security mission, DHS needs the ability to predict long-term changes in the composition and manufacturing of synthetic drugs and to automatically detect and track the physical presence of opioids/fentanyl, precursor materials used for illegal narcotics, and counterfeit pharmaceuticals from foreign or domestic sources.

DHS Mission Three: Administer the Nation’s Immigration System

Mission Three is achieved through the efficient and equitable administration of the U.S. immigration system and enforcement of U.S. immigration laws. Under this mission, DHS is responsible for adjudicating most applications and petitions for immigration benefits, maintaining the cohesiveness of immigration IT systems, and providing trustworthy and timely immigration, employment, and identity information to stakeholders. DHS is also committed to enforcing immigration laws while treating all involved with dignity and respect. Further, DHS is committed to preventing the exploitation of undocumented individuals and protecting the public from crimes of victimization and exploitation by strategically targeting and investigating individuals, businesses, and networks that engage in labor exploitation, including forced labor, a form of human trafficking. In supporting the Objectives under this mission, the IRD community is making critical investments in efficiency capabilities to streamline the administration of immigration benefit services and capability enhancements to improve processes related to detention, alternatives to detention, and U.S. interior and border removals. The following section outlines challenges, relevant current IRD activities, and future IRD capabilities for each Objective under this Mission.

Objective 3.1
Administer the Immigration System

Under this Objective, DHS must improve the efficiency of immigration services and reduce large backlogs while continuing to ensure benefits are granted only to those who qualify. To meet this challenge, DHS will upgrade technology and related processes used for the adjudication of immigration benefits, detection of fraud, and strengthening and streamlining of the vetting process for applicants.

Current IRD activities associated with this Objective include developing technology-supported tools, including AI, for immigration interview and documentation processes that will: enhance the ability to efficiently process immigration benefit applications/petitions; enhance the ability to identify fraudulent immigration applications/petitions; reduce applicant backlogs; improve staffing efficiency and retention; and improve customer throughput and satisfaction. Furthermore, the IRD community is working on identity management, preventing forgery and counterfeiting of official certificates and licenses in digital issuances of currently paper-based immigration credentials, digital issuances of work and/or task licenses, remote identity authentication, and the expansion of virtual interviewing capabilities. The IRD community is also developing integrated immigration modeling capabilities to capture complex immigration pathways, processes, and operating assumptions of the DHS and interagency partners involved. This will provide analytic rigor in supporting evidence-based decisions involving budgeting, operational planning, policy development, and program evaluation.

For mission success, future DHS IRD initiatives through FY 2030 will support additional digital adjudications of immigration benefit applications and petitions. Automated systems, improved algorithms, metadata analysis, and cyber software assurance and protection security measures will be needed to help officers identify fraudulently produced or altered documents that could indicate fraud, public safety, or national security concerns. The IRD community must also develop automated and real-time predictive analysis capabilities of projected future U.S. immigration patterns from global sources to fully ensure proper resourcing and asset allocations throughout the entire immigration lifecycle. Research into the root drivers of mass migration, including factors related to climate change and biothreats (including pandemics), is needed to properly inform predictive models.

Objective 3.2: Enforce U.S. Immigration Laws

DHS is working with the Departments of Health and Human Services, Justice, and State in an all-of-government effort to manage irregular migration across the Western Hemisphere. Against the backdrop of an immigration system that has not been reformed by Congress in decades, there are areas within immigration enforcement that will require system modernization and implementation of new technologies and/or methods to continue to safely and humanely enforce immigration laws and facilitate enforcement and removal operations for individuals who do not have a legal basis to stay in the United States.

Current IRD activities associated with this Objective include technology solutions for screening and vetting, detention, and alternatives to detention. Solutions on the alternatives to detention include using technology and case management to ensure improved compliance with release conditions, court hearings, and final orders of removal. End-to-end (E2E) models for enforcement and removal operations are also being developed to improve processes related to detention activities, alternatives to detention, and U.S. interior and border arrest removals. IRD is also supporting operators by enhancing communication and interaction capabilities, such as language translators that will automatically identify, translate (voice), and display the language being spoken in real-time to allow for two-way conversation. Finally, IRD is bolstering biometric capabilities to improve screening and vetting to ensure timely and accurate processing, including detection of face morphing or digital alterations to photos on passports or travel documents, while also safeguarding data protection and privacy.

For mission success, future DHS IRD initiatives through FY2030 will improve information sharing with other partners, allowing DHS to successfully perform our interior enforcement mission by identifying, locating, and targeting public safety threats while protecting privacy, civil rights, and civil liberties. All information sharing activities between various stakeholder sources must be trusted and enhanced cyber security measures must be taken to ensure private and sensitive information and intelligence remains protected against potential inadvertent release. Expedited processing and automated decision support capabilities are needed to protect communities from crime and potential attacks to the homeland. In addition, in-person or remotely processed automated fraudulent document detection and biometric and identity verification capabilities need to be enhanced to not only identify threats, but also to protect noncitizens from being exploited by groups or individuals seeking to take advantage of immigration status for their own financial gain. Finally, IRD will catalyze improved technologies for alternatives to detention.

DHS Mission Four: Secure Cyberspace and Critical Infrastructure

Mission Four is achieved through supporting the cybersecurity of federal civilian networks; strengthening the security and resilience of critical infrastructure; assessing and countering evolving cyber and emerging technology risks; and combatting cybercrime. IRD investments to meet the Objectives under this mission are being made to manage risk to FSLTT systems as well as private networks and infrastructure to ensure continued national security, economic security, and public health and safety. The DHS IRD community also invests in cybersecurity tools to identify and mitigate vulnerabilities, support services for cyber incident response and recovery, and risk management for critical infrastructure. The following section outlines challenges, relevant current IRD activities, and future IRD capabilities for each Objective under this Mission.

Objective 4.1: Support the Cybersecurity of Federal Civilian Networks

For this Objective, the volume of cyberattacks on Federal civilian networks is expected to increase as more government operations integrate information and communications technology. Given DHS's role as the lead for Federal Civilian Executive Branch (FCEB) cybersecurity, meeting this challenge requires Cyber Performance Goals, a suite of increasingly sophisticated, automated cybersecurity tools and processes to detect intrusions, protect against the volume of cyberattacks, and recover data if necessary, and the ability to provide better personnel training and testing of these tools and processes. DHS also needs improved cyber analytic capabilities to automate otherwise manual analysis of malware, gain information about adversaries, and improve risk assessments. Proactively sharing these risk assessments, mitigation tools, and best practices with Federal civilian agencies across the *.gov* domain will reduce risk and support essential operations. This includes improving supply chain risk management and preventing foreign adversary investment in U.S. hardware and software providers through the Committee on Foreign Investment in the United States (CFIUS).

Current IRD activities associated with this Objective are focused on expanding cybersecurity protections across FCEBs to protect the entire *.gov* environment, improving the cyber workforce's visibility into threats to federal networks, and providing tools to automate previously manual operations in threat identification and mitigation. EINSTEIN 3 Accelerated (E3A) uses classified information to detect and block traffic indicative of a cyberattack from federal networks and has been expanded to cover over 99% of FCEB users; when E3A is decommissioned, the next generation of systems (Protective DNS, which is live, and Protective Email, which is under development) leverage industry architectures and will also incorporate analytics. IRD is underway to route more traffic through a few, well-defended positions to more easily bring advanced cybersecurity tools and protections to bear against attempts to infiltrate networks.

DHS is exploring numerous uses of AI/ML to improve threat hunting, better utilize large and complex data sets, better query and correlate information related to cyber risk analysis, and enable security orchestration, automation, and response. AI systems themselves are being secured, which includes extensions of cybersecurity frameworks, as well as counter-adversarial machine learning. IRD focused on enhanced risk analysis, consequence analysis, and threat intelligence data capabilities will improve incident response times and threat and mitigation correlation. DHS is also enhancing software assurance by developing tools and techniques that ensure the security of applications within government environments, as well as examining software's composition and lifecycle to track usage, origin, unnecessary features that may be exploited, and any code bases that may not be secure.

For mission success, future DHS IRD initiatives through FY 2030 will prepare FCEB agencies for cyberattacks and be able to rapidly recover from a cyber incident to maintain mission continuity. This requires DHS to drive the adoption of modern, secure, and resilient technologies across federal networks. Every piece of hardware and software may contain vulnerabilities. To reduce the exploitation of those vulnerabilities, DHS must drive the disclosure and mitigation of critical cyber vulnerabilities. DHS needs next-generation architectures, computation, and decision-making capabilities to protect against those vulnerabilities, to include digital identity and continuous authentication tools to enable zero trust architectures with robust identity and identity-based security and access protocols. Each of those new tools will need protection throughout their lifecycle and supply chain.

Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure

Attacks on cyber and physical infrastructure have far reaching implications for homeland security. Increasingly, adversaries seek to exploit cyber vulnerabilities in physical infrastructure systems to inflict damage. To address this evolving threat, DHS must work with the private sector, interagency partners, and the Sector Risk Management Agencies to ensure that if a cyber or physical incident occurs, critical services remain in place in accordance with this Objective. DHS provides risk management support to owners and operators of critical infrastructure, using the National Critical Functions (NCFs) to frame the analysis of where risk is concentrated and then focus mitigation efforts. DHS provides services to mitigate risk throughout the lifecycle of critical infrastructure, from preventing vulnerabilities at their source through supply chain risk management to physical assessments of infrastructure. Most critical infrastructure is privately owned, so DHS utilizes public-private partnerships to improve security and resilience of the assets, entities, and systems that provide NCFs.

Current IRD activities associated with this Objective support the security and resilience across the sixteen (16) critical infrastructure sectors. Specifically, DHS is using IRD to prevent intrusion to critical networks, such as those for biometrics, law enforcement, maritime transportation, and the *.gov* enterprise. IRD is improving our understanding of the complex public and private sector linkages that comprise an infrastructure system and community to ensure that the stress of catastrophic events does not impede critical services.

DHS is investing in IRD to assist DHS and the critical infrastructure industry in analyzing and understanding threats, vulnerabilities, risk management strategies, costs, and trade-offs in risk management decisions. DHS is using IRD to support increased threat hunting and to conduct cyber vulnerability assessments. Finally, DHS is employing IRD to protect against the impacts of climate change and infrequent but potentially catastrophic events that have the potential to disrupt large portions of the US economy and infrastructure (e.g., a geomagnetic disturbance (GMD) (space weather) or an electromagnetic pulse (EMP)).

For mission success, future DHS IRD initiatives through FY 2030 will help DHS detect and prevent threats while also improving the security and resilience of and mitigating cascading attacks against critical infrastructure that NCFs rely on. Doing so will minimize the impact of attempts to infiltrate, exploit, disrupt, or destroy critical infrastructure systems, networks, and NCFs they enable. However, DHS cannot mitigate threats it does not see, which requires expanding its operational visibility of threats to critical infrastructure. DHS receives a massive amount of data from federal partners and private sector owners and operators that will require NLP capabilities to better correlate heavily structured cyber data with unstructured physical infrastructure security data. DHS will work to motivate software and hardware manufacturers to begin incorporating security-by-default that prioritizes security and strong controls to prevent the prevalence of exploitable vulnerabilities. DHS is also planning substantial future IRD to provide research and tools for event risk assessments; protection against impacts of climate change, EMP, and GMD; protection of position, navigation, and timing systems; public safety for ST-CP; testing of new telecommunications equipment; exploration of AI/ML to increase resiliency; testing and security of industrial control systems; and security for open-source software.

Objective 4.3:
Assess and Counter Evolving Cyber and Emerging Technology Risks

Under this Objective, DHS works to incorporate emerging threats and address risk identification and risk mitigation holistically into our efforts to secure critical infrastructure by addressing both current and emerging risks arising from new technologies. Cyber-related vulnerabilities in new technologies and products ranging from low earth orbit commercial communications satellites, AI/ML, consumer and industrial Internet of Things (IoT) devices, to automation, represent new attack vectors adversaries may use to target the homeland. Collaboration with government, industry, academia, and international partners to identify and remedy cyber vulnerabilities that threaten economic and national security is key, using a cross-sector risk management process that recognizes critical infrastructure is interconnected and an attack on one entity may not be limited to a single network or sector.

Current IRD efforts associated with this Objective focus on analysis of recent technology developments that introduce vulnerabilities among the HSE and developing mitigation measures to protect against the exploitation of those vulnerabilities. For example, DHS is using IRD to innovate threat hunting capabilities to identify new vulnerabilities on FSLTT networks while coordinating with industry partners to better understand threats to private networks. DHS is positioned to be at the forefront of innovation for public sector use cases for government use of responsible AI. DHS's research partners are tracking adversarial use of AI, to include cyberattacks, bots and other autonomous fake and/or malicious accounts and activity. IRD is improving the cybersecurity of the emergency communications ecosystem to mitigate the risk of cyberattacks negatively impacting public safety response (e.g., 911 services) or preventing first responders from effectively communicating with each other. Finally, IRD initiatives are assessing technology risk areas that can be used to close or mitigate identified risks.

For mission success, future DHS IRD initiatives through FY 2030 will support DHS identifying and institutionalizing the management of emerging and systemic risks *before* they pose threats to critical infrastructure. To provide accurate risk management, DHS needs better visibility into emerging and evolving risks, including how and when they may emerge and what impacts they may cause the nation (including threats to private networks and privately-owned critical infrastructure). DHS needs capabilities that provide cutting-edge research and proof-of-concept and successful evaluation of innovative infrastructure security and resilience across digital ecosystems. Finally, DHS operational units require the ability to query and correlate cyber risk information with physical and infrastructure risk as the prevalence of blended cyber/physical threats increases.

DHS must go beyond simply identifying emerging risks to providing tools and processes to mitigate the risks from emerging technologies before they are able to impact NCFs. Responses to threats from adversarial AI require new AI tools to detect and mitigate new activity at speed and scale. DHS must drive the adoption of security-by-default in the technology ecosystem so that software and hardware manufacturers prioritize security and strong controls that reduce the prevalence of exploitable vulnerabilities. Finally, DHS requires capabilities to better train the cyber workforce to be prepared for constantly evolving threats to FCEB and private networks.

Objective 4.4: Combat Cybercrime

DHS must continue to find ways to prevent, identify, and disrupt cyber-enabled criminal activity to meet the desired outcome under this Objective. This includes blunting the ability of TCOs to exploit the transnational and cross-jurisdictional nature of cyberspace for their criminal and financial ends. It also includes countering illicit finance whether it is via counterfeiting, fraud, money laundering, the use of illicit marketplaces, the improper use of virtual currencies, or ransomware. DHS must leverage Component expertise in countering cybercrime to protect children and vulnerable people from exploitation such as human trafficking and child sexual abuse material (CSAM).

Current IRD activities associated with this Objective are developing tools and processes to counter known technologies and tactics employed by criminals. This includes data that must be collected and analyzed so that criminals cannot mask ownership or movement of illicit currency.

For mission success, future DHS IRD initiatives through FY 2030 will support DHS countering criminals who are increasingly using new technologies and tactics to conduct crimes, mask responsibility, and transfer illicit gains. DHS needs technologies and tools that enable investigators to identify criminals attempting to use cryptocurrency and other digital assets to transport and launder money. Development of liveness checks and other countermeasures for combating real-time video or audio deepfakes (used for spoofing video conferences or calls) which can establish trust/authentication for illicit cybercrime activities are also needed. DHS must also prevent criminals from using new technologies to render evidence infeasible to recover, which hinders the prosecution of cybercrimes. Digital forensics and enhanced detection capabilities are needed to enable law enforcement to visualize data and analyze evidence more expeditiously to increase the effectiveness of disrupting or investigating usage of digital currencies and malicious software for criminal gain.

DHS also needs capabilities to reduce the prevalence and impact of cybercrimes. This requires reducing the number of vulnerabilities available for exploitation, so that malicious code does not make it into software supply chains. Capabilities to prevent network intrusions in the private sector, where non-state actors are using increasingly sophisticated attacks to steal intellectual property, insert ransomware, and resell valuable data, are vital. To ensure that our law enforcement Components are most effective in combatting cybercrime, DHS needs cybersecurity capabilities to protect law enforcement systems, vehicles and other equipment, and records. Finally, DHS law enforcement personnel require training to address the technological, social, and economic impacts of malicious cyber activities.

DHS Mission Five: Build a Resilient Nation and Respond to Incidents

Mission Five is achieved through coordinating federal response to incidents; strengthening national resilience; supporting equitable community recovery; and enhancing training and readiness of first responders. DHS IRD supports the Objectives under this mission by building capabilities to ready the nation to respond to and quickly recover from current and emerging threats and hazards across the homeland security mission space. This is best accomplished under the paradigm of *resilience*, which emphasizes identifying and confronting systemic risk, building redundancy into community lifelines, and raising the baseline of our security. Because disasters can affect communities disproportionately, IRD also supports discovering new and better ways to ensure equitable community recovery when tragedy does strike. Finally, IRD plays a critical role in ensuring that the nation's first responders are well-trained and equipped with the right tools to protect communities from complex and changing threats and hazards. The following section outlines challenges, relevant current IRD activities, and future IRD capabilities for each Objective under this Mission.

Objective 5.1:
Coordinate Federal Response to Incidents

DHS will be called upon to respond to increasingly complex, simultaneous, and interconnected incidents nimbly and decisively. Both the frequency and severity of natural hazards are projected to increase due to climate change. Biosecurity incidents are also expected to remain a persistent threat. In addition, man-made threats including targeted violence and cyber-attacks on critical infrastructure will increasingly necessitate multi-domain, cross-functional responses. Particularly when threats and hazards converge—for example, a cyber-attack during a major hurricane—disruptions and impacts are accentuated, operating environments become degraded, and DHS response capabilities can be strained. Finally, because incident response necessarily involves FSLTT entities—as well as the private sector which owns most of the nation's critical infrastructure—to be effective, DHS's incident response capabilities must be closely coordinated with our partners to meet the desired outcome of this Objective.

Current DHS IRD investments associated with this Objective focus on reducing incident response vulnerabilities by providing interoperable communications across operating environments, including low-cost, ubiquitous global satellite communications networks and multi-modal communications devices to provide cellular and mesh communications capabilities for operations and disaster response situations. Other IRD efforts seek to provide state and local communities access to new and emerging technologies and innovations which reduce risk, improve protective measures, optimize mitigation investments, and lower the costs of disasters. Finally, DHS has directed IRD resources towards coastal and maritime problem spaces, funding projects that support disaster response, search and rescue, and environmental incident management, including in environments and locales posing unique challenges such as the Arctic and coastal/island communities adversely affected by more intense storms and rising sea levels.

For mission success, future DHS IRD initiatives through FY 2030 will focus on enabling integrated, data-driven analysis, decision support, and communications for incident response across all key stakeholders and domains. This includes near real-time search and rescue capabilities, ideally over ever-wider areas; improved incident response times; and streamlined and optimized disaster recovery operations and assistance programs.

Objective 5.2: Strengthen National Resilience

Research indicates that damage, response, and recovery costs from disasters and other incidents fall dramatically when communities are resilient. Resilience is built when communities are thoroughly prepared for threats and hazards, with strong critical infrastructure systems that are calibrated to the risks of today and tomorrow. When disaster does strike, resiliency is also provided by the prior establishment of rapid response and sustainable recovery practices which are available for immediate deployment. Given an expected trajectory of more flooding, fires, drought, and extreme heat, climate change poses one of the top challenges in this space; climate resilience will be increasingly important to communities across the nation who will no longer enjoy “off seasons” for disasters. The implications of climate change are not limited to the United States: globally, environmental factors are expected to drive migration—with potential impacts to the homeland—as well as degrade agricultural production and food security worldwide.

Current DHS IRD investments associated with this Objective focus on improving coastal resilience, evaluating new solutions to reduce fatalities and property losses, expanding state and local first response capacities, and optimizing pre- and post- disaster grants programs. IRD resources are also currently channeled toward countering threats posed by unmanned systems, explosives and CBRNE threats, strengthening urban security (particularly the transportation sector), enhancing waterway management, and augmenting maritime hazardous spill response.

For mission success, future DHS IRD initiatives through FY 2030 will position the Department to: better forecast natural hazards and their impacts; prepare communities for more frequent and severe events through improved preparedness, response, and recovery infrastructure and practices—notably using affordable, game-changing technologies; strengthen supply chains; enhance collection, analysis, sharing, and employment of incident management data across DHS Components and with our state, local, tribal, and territorial partners; and augment coordination and communication with critical infrastructure sectors ahead of, during, and after an incident.

Objective 5.3:
Support Equitable Community Recovery

Disasters impact people and communities differently. Research indicates that disparities between geographic, demographic, political, historical, and cultural groups are key factors in both the impact of a disaster as well as its recovery timeline. Underserved communities experience differences in how well their homes have been adapted to mitigate against local hazards, how prepared they are to respond to disasters, and how quickly their communities are able to resume social and economic life after a major event—including through their ability to access federal recovery services. As a result, disasters worsen inequities already present in society. This challenge requires the nation to advance climate resilience and further increase equity in preparedness and response efforts to support communities disproportionately impacted by disasters in accordance with this Objective.

Current IRD investments associated with this Objective focus on improving community access to new and emerging technologies and innovations that streamline and optimize disaster recovery operations and assistance programs—including flood predictive analytic tools that reduce future flood fatalities and economic damages and advancements from geophysical, materials, self-healing, and regenerative sciences. Other research seeks new market innovations, policy options, and technology to improve risk reduction outcomes, advance social and environmental equity, and build resiliency in underserved communities. DHS has established community resilience testbeds with localities and the private sector to assess, evaluate, and innovate new approaches and technologies to disaster response, enhancing cooperation between federal, state, local, and private sector to spur innovation and implement new technologies.

For mission success, future DHS IRD initiatives through FY 2030 will support recovery efforts that facilitate effective communication with affected communities prior to and in the aftermath of a disaster, lower barriers to accessing federal assistance, and improve the customer experience for both disaster survivors and SLTT partners. IRD will identify and enhance scientifically sound sources of data on social equity to better support homeland security climate adaptation and disaster resilience efforts. This capability will allow DHS to address and mitigate identified gaps in federal recovery programs, advance equity, and improve disaster resilience outcomes.

Objective 5.4:
Enhance Training and Readiness of First Responders

First responders in communities across the nation provide critical emergency management services for communities and individuals affected by a complex mix of threats and hazards, making it vital that they are ready to respond in accordance with this Objective. The nation’s first responders must be able to address these evolving threats and hazards in a challenging sociopolitical operating environment. Capability building, to include investments and innovations that will allow them to conduct their missions more safely, effectively, and efficiently, is critical. While commercializing technology to fully meet these challenges is typically a lengthy process, developing near-term, innovative technologies that address high priority capability gaps identified by FSLTT first responders can ensure their safety, performance, and well-being.

Current IRD investments associated with this Objective focus on providing operators improved abilities to detect, prevent, and respond to threats and hazards. DHS is identifying high priority needs, developing prototype solutions, and conducting operational field assessments of and experimentation on next generation technologies to address gaps, with the goal of rapidly developing and transitioning technologies. A particular focus is on improving responder preparedness for the complexity of chemical, biological, radiological/nuclear, and explosive incident response and recovery operations.

For mission success, future DHS IRD initiatives through FY 2030 will expand threat and hazard surveillance, early warning and actionable information sharing, and prediction capabilities. These insights will be shared with first responders, reducing demands on their limited resources, especially in rural areas. Geolocation enhancements will enable position tracking of personnel on the incident scene while new tools for training and collaboration will allow large numbers of geographically dispersed first responders to collaborate and train simultaneously, repeatedly, and frequently in an experiential and realistic manner. To improve response, additional capabilities will assist law enforcement and response communities in safely dispersing large crowds, recognizing hazards, deterring violence, and applying less-than-lethal force when required. As a force multiplier, IRD-fostered technological enhancements will support first responders by reducing their cognitive loads, freeing officers to focus on their key missions. Finally, IRD will help address officer safety, wellness, and retention issues to ensure the vitality and sustainability of the nation's critical first responder community.

DHS Mission Six: Combat Crimes of Exploitation and Protect Victims

Mission Six is achieved through enhancing prevention using public education and training; identifying, protecting, and supporting victims and those at risk; and detecting, apprehending, and disrupting perpetrators. DHS IRD supports Objectives under this mission by building capabilities to prevent, identify, investigate, disrupt, and dismantle human trafficking, child sexual exploitation and abuse (CSEA) including CSAM and other exploitation-based crimes such as labor exploitation. Research is key both to understanding the dynamics of these crimes as well as uncovering methods to better survey existing DHS data holdings that hold insights about victims, perpetrators, and those at risk. With child sexual exploitation and abuse exploding online and increasingly enabled by end-to-end encryption, new approaches to detection and deterrence of illicit activity are critical. The following section outlines challenges, relevant current IRD activities, and future IRD capabilities for each Objective under this Mission.

Objective 6.1: Enhance Prevention through Public Education and Training

Under this Objective, preventing crimes of exploitation requires robust education and training for both internal and external stakeholders. Internally, many DHS operators have roles that require interactions with the public; proper training is needed to understand risks and spot indicators of exploitation to identify and report potential victims and perpetrators. DHS's FSLTT partners have myriad additional public contacts and thus added opportunities to advance prevention. In both cases, given the high volume of interactions, information, tools, and techniques that can rapidly assist an operator with identifying potential victims and perpetrators are required. Finally, DHS needs to optimize its public education efforts to raise awareness around best practices to identify and prevent human trafficking, CSEA or other forms of child exploitation including labor exploitation, and the related illicit financial activity associated with these crimes.

Current DHS IRD investments associated with this Objective focus on assessing DHS' prevention initiatives and identifying opportunities to leverage research to improve outcomes. IRD is also evaluating the effectiveness of the DHS Blue Campaign and its potential applicability to other education and awareness tools, programs, and initiatives.

For mission success, future DHS IRD initiatives through FY 2030 will focus on exploring the validity of using prevention frameworks to reduce and mitigate the incidence of offenses. In concert with human trafficking experts, survivors, behavioral clinicians, and prevention practitioners, promising practices in public education and training will be identified and shared with stakeholders. DHS tools and training will be made available to other countries to deter transnational exploitation while robust international R&D partnerships will catalyze prevention capabilities development for multiple stakeholders. Finally, DHS will pursue robust collaboration with the technology industry to combat human trafficking and forced labor in the supply chain and prevent and stop online CSEA.

Objective 6.2: Identify, Protect, and Support Victims

As DHS pursues a trauma-informed and victim-centered approach to minimize additional trauma endured by many victims, mitigate any undue penalization, and provide needed stability and support to victims of trafficking and exploitation, several challenges emerge under this Objective. Positive identification of victims can be difficult, especially with people of differing ages, particularly children; accurate identification of locations where victimization takes place is similarly problematic. The sheer volume of digital data surrounding these crimes can make recognizing indicators, signatures, pathways, and potential overlaps of victimization difficult. Finally, DHS operators addressing heinous human trafficking, CSEA and CSAM, and other exploitation-based crimes including labor exploitation may themselves experience trauma or other job-related stressors, affecting morale, well-being, and retention.

Current DHS IRD investments associated with this Objective focus on improving digital forensics to identify victims. With hundreds of millions of child exploitation images online and myriad livestreams, operators need tools that can dramatically speed up the process of initial triage and the subsequent forensic deep dive analysis of digital imagery. Such tools will amplify an agent's effectiveness while drastically limiting their exposure to traumatizing material. DHS is also using IRD to counter those engaged in human trafficking, CSEA, or CSAM by improving victim identification, analysis of networks engaged in these activities, and improving exploitation of evidence gathered in investigations. IRD is also examining options for secure computing platforms and/or investigative tools that will increase victims' privacy.

For mission success, future DHS IRD initiatives through FY 2030 will focus on capabilities to quickly and positively identify every victim, using accurate biometric identification technology (especially for children, a current gap), recognition algorithms, and AI/ML. Architectures and prototypes will enable law enforcement to find criminal behavior on social media and livestream platforms while providing data analysis near real time. IRD will support effective tools and methods to minimize exposure to traumatic material and address the personal toll working in this environment imposes on DHS personnel addressing human trafficking, CSEA, CSAM, and other exploitation-based crimes. DHS must use its expertise in countering cybercrime to protect children and vulnerable people from exploitation such as human trafficking and child sexual abuse. DHS will also have the tools to unmask goods and supply chains that that may be tied to forced labor in foreign countries. Research insights will be used to minimize additional trauma, mitigate undue penalization, and stabilize and support victims.

Objective 6.3:
Detect, Apprehend, and Disrupt Perpetrators

Perpetrators of human trafficking, CSEA including CSAM, and other exploitation-based crimes including labor exploitation often operate clandestinely, leveraging tools that offer cyberspace anonymity and changing their techniques, tactics, and procedures to evade detection, posing challenges under this Objective. Apprehension and disruption efforts are also challenged by the volume of these crimes and the scope and complexity of transnational criminal networks.

Current DHS IRD investments associated with this Objective focus on tools and technologies to combat perpetrators tactics to avoid detection, including those who use anonymous browsing or move their internet servers overseas to evade law enforcement. IRD is also improving detection, analysis, and understanding of exploitation and conducting gap analyses to identify aspects of exploitation (victims or perpetrators) in greatest need of empirical research. Guided by a long-term exploitation research agenda, IRD will fill knowledge gaps related to labor trafficking in the United States. DHS collaborates on this Objective with Five Eyes countries, including through the Combatting Child Exploitation Network. The network is part of the 5 Research and Development (5RD) Council, an R&D-focused forum that brings together national security leadership and technical expert networks to address shared challenges across the five countries: the United States, Australia, Canada, New Zealand and the United Kingdom.

For mission success, future DHS IRD initiatives through FY 2030 will advance the labor trafficking research agenda by focusing on building research and data collection efforts to better understand the scope and dynamics of human trafficking. Insights will inform the development of more effective training, prevention, and intervention strategies. IRD will support new capabilities to collect, link (internally and with external organizations such as non-governmental organizations) and analyze data (including non-structured data) for investigations of exploitation. This process will be augmented by using analytical exploitation (AI/ML). Seamless connectivity between agencies, coupled with immediate information sharing and connection to victims, suspects, and cases, will lead to more victims being identified and children rescued. New approaches and technologies will mitigate the challenge of E2E providing a haven for child predators. Finally, DHS will develop IRD-driven capabilities to support law enforcement in identifying victims and prosecuting perpetrators of exploitation, with the ultimate goal of disrupting networks, deterring perpetrators, and reducing the incidence of these crimes.

STRATEGIC PRIORITY RESEARCH AREAS

Cross-Cutting IRD for Mission Success

IRD is a critical tool for the Department to build the capabilities needed to achieve desired outcomes across the DHS mission space. Common trends across future capabilities reveal opportunities for DHS to optimize its IRD investments by applying them in a cross-cutting manner to deliver future capabilities across various DHS Missions and Objectives. To this end, the Department developed the concept of a ***Strategic Priority Research Area (SPRA)***, a cross-cutting assembly of enduring scientific efforts which provide a means for addressing priority needs across multiple HSE mission areas.

SPRAs will significantly strengthen the DHS enterprise by enabling the following anticipated outcomes:

- Accurate forecasts of emerging and future threats and hazards provide early warning to operators, strengthening preparedness, deterrence, and response.
- Reduce risk to the homeland by detecting threats and hazards in a timely manner with the highest level of confidence to enable the HSE to rapidly respond.
- Respond quickly and decisively during homeland security incidents to reduce their impact; improve community and workforce resilience and recovery.
- DHS operators have at hand the high-quality information and analysis they need to make effective decisions.
- DHS IRD investments are optimized to meet strategic challenges and improve mission operations while ensuring that constitutional, statutory, regulatory, policy, and other requirements are appropriately incorporated, such as those for safeguarding privacy, civil rights, and civil liberties and involving human subjects research and export controls.

SPRAs also provide opportunities to strengthen existing and establish new partnerships with industry, academia, other federal agencies, and international entities in areas of shared interest. Based on analysis, the following are eight (8) SPRAs that will organize and synergize DHS's IRD initiatives through FY 2030:

Strategic Priority Research Areas	*DHS Mission Alignment*					
	1	2	3	4	5	6
Advanced Sensing	✓	✓	✓	✓	✓	
Artificial Intelligence and Autonomous Systems	✓	✓	✓	✓	✓	✓
Biotechnology	✓	✓	✓	✓	✓	
Climate Change	✓	✓	✓	✓	✓	
Communications and Networking	✓	✓	✓	✓	✓	✓
Cybersecurity	✓	✓	✓	✓	✓	✓
Data Integration, Analytics, Modeling and Simulation	✓	✓	✓	✓	✓	✓
Digital Identity and Trust	✓	✓	✓	✓	✓	✓

Advanced Sensing SPRA

All DHS operations rely on the ability to detect, track, monitor, and identify activities, goods, people, or threats across different environments—including air, land, and maritime borders, maritime, wildlands, urban, transportation sectors, space, etc.—and in different event situations and venues ranging from daily operations to disaster response. To effectively sense a threat requires a foundational understanding of the characteristics of the threat that enable it to be sensed (oftentimes referred to as a signature) and the ability to determine that those characteristics are present through an individual sensor or sensing system. The ***Advanced Sensing SPRA*** will explore IRD pathways for next generation sensor capabilities with enhanced performance such as providing real-time results across a broad spectrum of non-biological threats with the highest levels of reliability and accuracy without disrupting operations. For biological threat detection, refer to the Biotechnology SPRA section in this document. The Advanced Sensing SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.4) Alternative approaches to detection that leverage non-traditional, non-biological threat signatures; next generation countermeasures for food, agriculture, and veterinary sectors.
- (DHS Mission Two, Objective 2.1) Detection capabilities to provide persistent domain awareness and enhance detection, tracking, identification, and classification.
- (DHS Mission Two, Objective 2.2) Detecting concealed non-biological threat materials (e.g., explosives and chemical) in airport scanning systems.
- (DHS Mission Three, Objective 3.2) Improved technologies for alternatives to detention.
- (DHS Mission Four, Objective 4.2) Expanding operational visibility of non-biological threats to critical infrastructure.
- (DHS Mission Five, Objective 5.4) Geolocation enhancements to enable position tracking of personnel on the incident scene; determining the presence of non-biological threats to give LE insight into dynamics of a large crowd.

Artificial Intelligence and Autonomous Systems SPRA

According to 15 U.S.C. 9401(3), the term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. In semi or fully autonomous systems, AI receives input (e.g., through sensors), produces an output internal to the system (decision), and then acts on that output (action) to affect the external world state. An autonomous system, particularly fully autonomous, will require AI in both the sensing and deciding cycles. Adversarial AI, described as attacks against AI-based systems, and adversarial use of AI to attack an AI-based system, is a known risk/threat in this area. AI includes subfields such as machine learning, natural language processing, computer vision, and predictive analytics. The ***Artificial Intelligence and Autonomous Systems SPRA*** will explore IRD pathways to applying capabilities across these subfields to enhance DHS operations. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.3) Automated threat detection to safely screen people and their belongings in ST-CP; mechanisms for reducing burden on those doing the protecting through process automation and effective training.
- (DHS Mission One, Objective 1.4) Autonomous detection and tracking of threats while simultaneously monitoring or responding to multiple targets at once; advanced algorithms such as ML for enhanced operator decision making.
- (DHS Mission Two, Objective 2.1) Autonomy of detection capabilities to provide persistent domain awareness and enhance detection, tracking, identification, and classification.
- (DHS Mission Two, Objective 2.3) Automated digital media exploitation and forensic alerting of nefarious TCO cyber activity; automatically detect and track the physical presence of opioids/fentanyl, precursor materials used for illegal narcotics, and counterfeit pharmaceuticals from foreign or domestic sources.
- (DHS Mission Three, Objective 3.1) Automated and real-time predictive analysis capabilities of projected future U.S. immigration patterns from global sources.
- (DHS Mission Three, Objective 3.1) Automated detection of immigration fraud.
- (DHS Mission Three, Objective 3.2) Automated decision support capabilities to protect communities from crime and potential attacks to the homeland; in-person or remotely processed automated fraudulent document detection and biometric and identity verification capabilities.
- (DHS Mission Four, Objective 4.1) Increasingly sophisticated, automated cybersecurity tools and processes to protect against the expected increase in volume of cyberattacks; improved cyber analytic capabilities to automate otherwise manual analysis of malware, gain information about adversaries, and improve risk assessments.
- (DHS Mission Four, Objective 4.2) NLP capabilities to better correlate heavily structured cyber data with unstructured physical infrastructure security data; NLP for workflow enhancement, automated tool deployment, software/code analysis, and disinformation.
- (DHS Mission Four, Objective 4.3) Defense against adversarial AI; exploration of AI/ML to increase resiliency.
- (DHS Mission Five, Objective 5.1) AI to improve rapid damage assessment, wildfire prediction, ignition detection, and resource mobilization.
- (DHS Mission Five, Objective 5.2) AI to enhance just-in time disaster-related training and education.
- (DHS Mission Five, Objective 5.3) AI to enhance the customer experience and make assistance easier to access and navigate while detecting and preventing fraud.

- (DHS Mission Five, Objective 5.4) AI to predict large crowd dynamics to queue LE deployments; autonomous systems for crowd surveillance as a force multiplier for LE when required to improve responses to violent or dangerous incidents.
- (DHS Mission Six, Objective 6.2) AI/ML to identify victims quickly and positively, unmask goods in supply chains tied to forced labor.

Biotechnology SPRA

The biological threat landscape continues to evolve, along with rapidly changing complexities in the geopolitical landscape that could impact biological defense. DHS must be on the cutting edge of research and development to understand these threats to the homeland and be able to counter them, whether through threat awareness, preparedness, detection, mitigation, response, or recovery. The same technologies and developments which may increase the magnitude of biological threats can also be leveraged to address them. DHS must understand a broader array of threats, seek detection and response options that are agnostic to the agent of concern, and integrate new technologies, such as machine learning and artificial intelligence, to aid human decision making and speed identification and response to biological threats, whether enduring or emerging. The ***Biotechnology SPRA*** will explore IRD pathways to achieve these needs. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.1) Developing a platform and/or integrating with existing systems to enable knowledge products and tools to be effectively shared with the wider HSE to promote communication, scientific and medical understanding, and risk awareness of biological threats.
- (DHS Mission One, Objective 1.3) Understand the potential biological threats that could have a small-scale impact on individuals and/or working animals and ways to detect and mitigate them and develop methods to conduct continuous wide-area biological threat monitoring.
- (DHS Mission One, Objective 1.4) Fill critical knowledge gaps on biological threat agents and develop enhanced biological threat detection technologies, including near real-time detection agent-agnostic approaches.
- (DHS Mission One, Objective 1.4) Develop improved modeling of public health impacts from known and unknown biological threats to inform the procurement and/or development of medical countermeasures and the implementation of science-based non-pharmaceutical interventions.
- (DHS Mission Two, Objective 2.1) Automatically share biothreat information across stakeholder communities in all domains seamlessly.
- (DHS Mission Three, Objective 3.1) To enhance predictive models, improved understanding of the relationship between biothreats (including pandemics) and mass migration.
- (DHS Mission Four, Objective 4.2) Assist critical infrastructure industry partners in analyzing and understanding biological threats, vulnerabilities, risk management strategies, costs, and trade-offs.
- (DHS Mission Four, Objective 4.4) Technologies and tools that enable investigators to identify malign actors attempting to proliferate bioagents and biotechnologies of concern.
- (DHS Mission Five, Objective 5.1) Integrated, data-driven analysis, decision support, and communications for bioincident prevention and incident response across all key stakeholders and domains.
- (DHS Mission Five, Objective 5.2) Enhance collection, analysis, sharing, and employment of incident management data across DHS Components and partners; augment coordination and communication with critical infrastructure sectors ahead of, during, and after a bioincident.
- (DHS Mission Five, Objective 5.3) Facilitate effective communications with affected communities prior to and in the aftermath of a biological attack.
- (DHS Mission Five, Objective 5.4) Expand biological threat and hazard surveillance, early warning and actionable information sharing, and prediction capabilities with first responders and other SLTT stakeholders.

Climate Change SPRA

Climate change is causing rising sea levels, increased temperatures, and changing weather patterns, resulting in more droughts, floods, hurricanes, wildfires, and extreme heat. This trend directly affects the HSE on multiple mission fronts. Changing weather patterns impact the nation's agricultural sector. The nation faces increased loss of lives, infrastructure damage, and economic costs due to natural disasters driven by climate change. DHS must strengthen climate adaptation and resilience to reduce disruptions and mitigate risks to critical infrastructure from climate change, improve social and environmental equity in climate resilience, enhance the resilience of critical information and communication technology, and promote solutions for reducing carbon emissions. The ***Climate Change SPRA*** will explore IRD avenues to achieve these activities. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.4) Predict and rapidly detect pathogens resulting from impacts of changing weather patterns on the food and agricultural sector.
- (DHS Mission Two, Objective 2.2) Predict and detect maritime hazards such as icebergs and inclement weather (e.g., heavy fog) to enhance prevention.
- (DHS Mission Three, Objective 3.1) Research into the root drivers of mass migration, including factors related to climate change, to properly inform predictive models.
- (DHS Mission Four, Objective 4.2) Understanding impacts of climate change on critical infrastructure to enhance resilience.
- (DHS Mission Five, Objective 5.1) Research to support federal response to concurrent incidents with cascading impacts, which are being driven or exacerbated by climate change.
- (DHS Mission Five, Objective 5.2) Better forecast natural hazards and their impacts; prepare communities for more frequent and severe events through improved preparedness, response, and recovery infrastructure and practices.
- (DHS Mission Five, Objective 5.3) Identify and enhance scientifically sound sources of data on social equity to better support homeland security climate adaptation and disaster resilience efforts.
- (DHS Mission Five, Objective 5.4) Development of capabilities to address the expanding Wildland Urban Interface and the firefighters who respond to incidents there.

Communications and Networking SPRA

Communications and networking across the HSE are vital to facilitate the information sharing needed to effectively carry out the DHS missions. The communications ecosystem includes both terrestrial (e.g., narrowband, broadband, High Frequency) and non-terrestrial (e.g., undersea, aerial, space) solutions and technologies such as 5G/XG, Smart Cities, Internet of Things, and smart devices; this ecosystem is continuously evolving. DHS must enhance communications and network capabilities, while maintaining security and resiliency, using advanced technologies. Increasingly robust communications capabilities will enable more effective information sharing and collaboration between humans and technologies but will also provide an expanded attack surface for adversaries to detect and affect the resilience of our operations. The ***Communications and Networking SPRA*** will explore IRD avenues to meet these challenges. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.1) Domain-agnostic information sharing across various classification levels in real time; highly available and resilient critical communications, services, and information sharing capabilities; increase sharing of threat-related information with the international community.
- (DHS Mission Two, Objective 2.1) Automatically analyze, communicate, and share information across stakeholder communities in all domains seamlessly.
- (DHS Mission Two, Objective 2.2) Real-time communication infrastructure and capabilities in remote maritime environments to effectively safeguard transportation systems, protect against illicit activity, and prevent against maritime hazards, such as icebergs and inclement weather (e.g., heavy fog).
- (DHS Mission Two, Objective 2.3) Seamless integration of interagency and international intelligence sharing framework capabilities on TCO activities to target, identify, and dismantle criminal networks.
- (DHS Mission Three, Objective 3.2) Improved information sharing with other partners to identify, locate, and target public safety threats while protecting privacy, civil rights, and civil liberties.
- (DHS Mission Four, Objective 4.3) Research of innovative infrastructure security and resilience for IoT devices.
- (DHS Mission Five, Objective 5.1) Integrated, data-driven analysis, decision support, and communications for incident response across all key stakeholders and domains, to include near real-time search and rescue.
- (DHS Mission Five, Objective 5.2) Enhanced collection, analysis, sharing, and employment of incident management data across DHS Components and partners; augment coordination and communication with critical infrastructure sectors ahead of, during, and after a threat or hazard.
- (DHS Mission Five, Objective 5.3) Facilitate effective communications with affected communities prior to and in the aftermath of a disaster.
- (DHS Mission Six, Objective 6.1) Catalyze prevention capabilities development for crimes of exploitation through robust international partnerships and information sharing.

Cybersecurity SPRA

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access, denial of service, or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. The increasing reliance on complex data, technology, communication, and interconnectivity has changed and expanded vulnerabilities and increased the potential risk to governmental, citizen services, and critical infrastructure continuity. Operational assurance in an increasingly digitally integrated environment such as the DHS of today and into tomorrow requires resiliency across data, software, hardware, and communications networks. The ***Cybersecurity SPRA*** will endeavor to explore achieving this with IRD. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.1) Domain-agnostic information sharing across various classification levels in real time; readily available and highly resilient critical communications, services, and information sharing capabilities.
- (DHS Mission Two, Objective 2.1) Enhanced software and network security provisions to prevent malicious cyber influences and maintain data integrity.
- (DHS Mission Two, Objective 2.2) IT systems requiring fully protected capabilities to protect from cyber-attacks to ensure robust supply chain risk management, information sharing, policy/regulation development, and enforcement for the MTS.
- (DHS Mission Two, Objective 2.3) Automated digital media exploitation and forensic alerting of nefarious TCO cyber activity.
- (DHS Mission Three, Objective 3.1) Cyber software assurance and protection security measures to identify fraudulently produced or altered documents in immigration system filings.
- (DHS Mission Three, Objective 3.2) Enhanced cyber security measures to ensure private and sensitive information and intelligence remains protected against potential and inadvertent release.
- (DHS Mission Four, Objective 4.1) Adoption of modern, secure, and resilient technologies—including "Secure by Design" and "Secure by Default" technologies---across federal networks; next-generation architectures, computation, and decision-making capabilities to protect against critical cyber vulnerabilities; increasingly sophisticated, automated cybersecurity tools and processes to protect against the volume of cyberattacks and recover if necessary.
- (DHS Mission Four, Objective 4.2) Improve the security and resilience of and mitigate cascading attacks against critical infrastructure that NCFs rely on.
- (DHS Mission Four, Objective 4.3) Query and correlate cyber risk information with physical and infrastructure risk as the prevalence of blended cyber/physical threats increases; better train the cyber workforce to be prepared for constantly evolving threats to FCEB and private networks.
- (DHS Mission Four, Objective 4.4) Cybersecurity capabilities to protect law enforcement vehicles; training to address the technological, social, and economic impacts of malicious cyber activities; enhanced detection and digital forensics tools to disrupt or investigate usage of digital currencies and malicious software for criminal gain.
- (DHS Mission Five, Objective 5.2) Ensuring integrity and availability of incident management data.
- (DHS Mission Six, Objective 6.3) Cyber analytics and forensics capabilities to detect and disrupt criminal communications and operations in cyberspace.

Data Integration, Analytics, Modeling and Simulation SPRA

Data is a value or set of values that provides a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means. Every day, DHS collects and uses data to execute our mission areas. Beyond its internal holdings, integrating multiple external data sources—under appropriate privacy and policy guidelines—can create an enriched data environment for DHS. This environment can be leveraged across mission sets to improve performance and operations. Data analytics is used to extract insights, patterns, inform conclusions, and support decision making from raw data sets. Within DHS, modeling and simulation is defined as a discipline that comprises the development and/or use of models and simulations and can be used to predict different operational outcomes. The outputs from these approaches are only as good as the data being consumed, leading to the need for an improved data ecosystem in DHS. The *Data Integration, Analytics, Modeling and Simulation SPRA* will endeavor to explore achieving this with IRD. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.3) Layered and integrated capability with automated threat detection to safely screen people and their belongings for potential threat materials and contraband in ST-CP without impacting the speed of travel.
- (DHS Mission One, Objective 1.4) Data integration and analytics to address multiple targets at once; modeling and simulation to gauge the ability of existing sensors to detect threats.
- (DHS Mission Two, Objective 2.1) Data integration and analytics capabilities that enable cross-domain data flows in a timely manner to provide actionable information for predicting potential illicit activity and informing decision making.
- (DHS Mission Two, Objective 2.3) Analytics to counter money laundering of specified unlawful activities beyond drug smuggling, including terror financing, financial fraud, human trafficking, export violations and sanctions violations; robust predictive analytics and forecasting using cutting-edge methods, agent-based models, and game theory to remain ahead of criminal actions, gang activities, and threats before they reach the homeland.
- (DHS Mission Three, Objective 3.1) Mature development of integrated immigration modelling capabilities to capture complex immigration paths, processes, and operating assumptions of the DHS and interagency partners involved to provide analytic rigor in supporting evidence-based decisions involving budgeting, operational planning, policy development, and program evaluation.
- (DHS Mission Four, Objective 4.4) Technologies and tools that enable investigators to identify criminals attempting to use cryptocurrency and other digital assets to transport and launder money.
- (DHS Mission Five, Objective 5.1) Integrated, data-driven analysis, decision support, and communications for incident response across all key stakeholders and domains.
- (DHS Mission Five, Objective 5.2) Modeling and simulation to better forecast natural hazards and their impacts; enhanced collection, analysis, sharing, and employment of incident management data across DHS Components and with partners.
- (DHS Mission Five, Objective 5.4) Modeling and simulation of large crowd disturbances to assist LE and response communities.
- (DHS Mission Six, Objective 6.2) Data analysis in real time of social media and livestream platforms to find criminal behavior.

Digital Identity and Trust SPRA

In today's increasingly digital world, trust is a key factor to ensure security. Maintaining the provenance, confidentiality, integrity, and availability of data is critical to transact with trust and maintain privacy across interconnected services, devices, and users. Digital identity is used to verify the identity of entities (natural person, non-person). The ability to establish and verify an individual's identity using asserted identity and biometric information enables the Department to perform risk-based decision making that is tailored to the individual. Digital trust is critical to verifying the validity of data, maintaining privacy, and ensuring data integrity across multiple platforms and applications. The ***Digital Identity and Trust SPRA*** will explore IRD opportunities to achieve this while ensuring approaches do not diminish privacy, civil rights, and civil liberties of persons. This SPRA is expected to make impacts towards delivering the following future capabilities across DHS Missions and Objectives:

- (DHS Mission One, Objective 1.2) Multi-layered screening and vetting architectures and identity technologies to prevent terrorist travel.
- (DHS Mission One, Objective 1.3) Increasingly accurate biometric capabilities to improve identity validation and verification of people accessing secure Federal facilities or other sensitive sites while also safeguarding privacy.
- (DHS Mission Two, Objective 2.1) Privacy-enhancing encryption capabilities to support information sharing; use of the information in a seamless interoperable communications network.
- (DHS Mission Two, Objective 2.2) Real-time, walk-by credential authentication and fraudulent document detection to improve security for an airport passenger's curb-to-gate experience.
- (DHS Mission Three, Objective 3.1) Prevention of forgery and counterfeiting of official certificates and licenses in digital issuances of currently paper-based immigration credentials, digital issuances of work and/or task licenses, and remote identity authentication for citizenship applications, which includes facial recognition and virtual interviewing capabilities.
- (DHS Mission Three, Objective 3.2) Biometric and identity verification enhancements to not only identify threats, but also to protect noncitizens from being exploited by groups or individuals seeking to take advantage of immigration status for their own financial gain.
- (DHS Mission Four, Objective 4.1) Digital identity and continuous authentication tools to enable zero trust architectures with robust entity and identity-based security and access protocols.
- (DHS Mission Four, Objective 4.4) Technologies and tools that enable investigators to identify criminals attempting to use cryptocurrency and other digital assets to transport and launder money.
- (DHS Mission Five, Objective 5.2) Ensuring that accurate and timely identity information is available for incident management and response.
- (DHS Mission Six, Objective 6.3) Improving accuracy of biometric identification technology (especially for children) to identify victims of crimes of exploitation quickly and positively.

CONCLUSION

The landscape of threats and hazards that the homeland faces today is diverse, complex, and evolving. DHS must stay ahead of this strategic environment by reducing the nation's risk from homeland security threats and hazards and avoiding technological surprise. This Strategic Plan sets a course for the Department to realize this vision by FY 2030. The Plan offers a pathway to bolster the efficiency and effectiveness of DHS's critical homeland security missions through improved and better coordinated IRD investments.

The eight (8) Strategic Priorities Research Areas (SPRAs) identified in the Plan are central to this effort. By focusing and articulating key research thrusts, the SPRAs will improve internal DHS collaborations and serve as a demand signal to industry, interagency, academia, and international collaborators on future partnerships and collaborations. These SPRAs will also significantly strengthen the DHS enterprise's ability to anticipate, prepare for, detect, deter, mitigate, and respond to threats and hazards through high-quality, readily available information while protecting privacy, civil rights, and civil liberties and adhering to applicable laws, regulations, guidelines, policies, best practices, and DHS Management Directives and Instructions, such as those for human subjects research and export controls.

DHS will implement this Plan in concert with its key internal and external stakeholders over the next seven fiscal years. In close collaboration with the Department at large and the IRDC Council in particular, S&T will engage in a series of implementation activities. These will include extensive industry partner engagement to communicate the Department's IRD priorities, as articulated in the Plan.

DHS will convene a series of internal cross-Departmental working groups organized around the SPRAs to map, coordinate, and amplify current and future research initiatives within each SPRA to develop IRD planning assessments, roadmaps, and/or agendas. In concert with OCFO, the IRDC Council will ensure that resourcing decisions about enterprise-wide IRD investments over the FY 2026 - FY 2030 and, as applicable, subsequent budget cycles are aligned with the priorities identified in the Plan. Finally, as a living document, the Plan will be updated and revised as threats and hazards, technologies, and/or DHS missions evolve.

APPENDICES

List of Acronyms

Acronym	Definition
5RD	5 Research and Development (a five-country (United States, Australia, Canada, New Zealand and the United Kingdom), R&D-focused forum that brings together national security leadership and technical expert networks to address shared challenges and provide scientific support to Ministerial level objectives).
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine Learning
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CFIUS	Committee on Foreign Investment in the United States
CSAM	Child Sexual Abuse Material
CSEA	Child Sexual Exploitation and Abuse
CY	Calendar Year
DHS	Department of Homeland Security
DVE	Domestic Violent Extremism
E2E	End-to-End
E3A	EINSTEIN 3 Accelerated
EMP	Electromagnetic Pulse
FCEB	Federal Civilian Executive Branch
FSLTT	Federal, State, Local, Tribal, and Territorial
FY	Fiscal Year
GMD	Geomagnetic Disturbance
HSE	Homeland Security Enterprise
IoT	Internet of Things
IRD	Innovation, Research, and Development
IRDC	Innovation, Research, and Development Coordination
IT	Information Technology
LE	Law Enforcement
LEO	Law Enforcement Officer
ML	Machine Learning
MTS	Marine Transportation System
NCF	National Critical Functions
NDAA	National Defense Authorization Act
NLP	Natural Language Processing
NSSE	National Special Security Events
OMB	Office of Management and Budget
POE	Port Of Entry

PPBE	Planning, Programming, Budgeting, and Execution
R&D	Research and Development
RAP	Resource Allocation Plan
S&T	Science and Technology Directorate
SEAR	Special Event Assessment Rating
SPRA	Strategic Priority Research Area
ST-CP	Soft Targets and Crowded Places
TCO	Transnational Criminal Organization
U.S.	United States

References

Critical and Emerging Technologies List Update, released February 7, 2022; see https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

Department of Homeland Security Priorities, released February 3, 2023; see https://www.dhs.gov/priorities

Executive Order on the Safe, Secure, and Trustworthy Development and use of Artificial Intelligence, released October 30, 2023; see https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

National Security Memorandum on Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security, released October 18, 2022; see https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/18/national-security-memorandum-on-countering-biological-threats-enhancing-pandemic-preparedness-and-achieving-global-health-security/

National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture, released November 10, 2022; see https://www.whitehouse.gov/briefing-room/presidential-actions/2022/11/10/national-security-memorandum-on-on-strengthening-the-security-and-resilience-of-united-states-food-and-agriculture/

Office of Management and Budget (OMB) Circular A-11, Part 6, Section 230, "Agency Strategic Planning;" see https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Science and Technology Directorate Research Agenda, released June 9, 2023; see https://www.dhs.gov/sites/default/files/2023-06/23_0609_st_tcd_research_agenda_r5_508.pdf

The Third Quadrennial Homeland Security Review, released April 20, 2023; see https://www.dhs.gov/sites/default/files/2023-04/23_0420_plcy_2023-qhsr.pdf

U.S. Department of Homeland Security Artificial Intelligence Strategy, released December 3, 2020; see https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf.

U.S. Department of Homeland Security Innovation, Research, and Development Coordination Implementation Guidance. February 15, 2023. Not available to the general public.