Soft Target Engineering to Neutralize the Threat Reality

A Department of Homeland Security Center of Excellence

Year 1 Annual Report Narrative
November 1, 2021 - June 30, 2022

Submitted by
Northeastern University
August 31, 2022

Soft Target Engineering to Neutralize the Threat Reality

Soft target Engineering to Neautralize the Threat Reality

A Department of Homeland Security Center of Excellence

Year 1 Annual Report Narrative
November 1, 2021 - June 30, 2022

Submitted by Northeastern University
August 31, 2022

Lead Partner: Northeastern University

Other Academic Partners:
Boston University • Rensselaer Polytechnic Institute • Rutgers University • Tufts University •
University at Buffalo • University of Florida • University of Notre Dame •
University of Puerto Rico at Mayagüez • University of Rhode Island • University of Southern California

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 22STESE00001-01-00. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Table of Contents

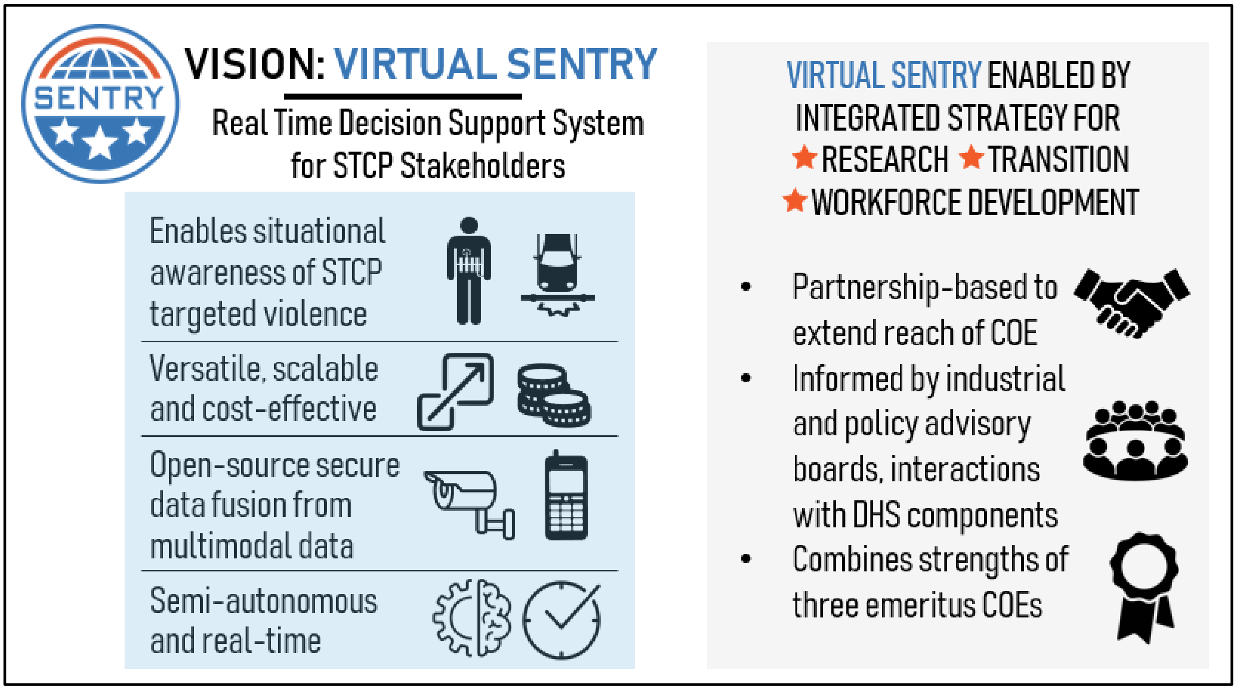
This page intentionally left blank.

Section 1: SENTRY Overview and Year 1 Highlights

1.1 SENTRY OVERVIEW

The SENTRY (Soft-target Engineering to Neutralize the Threat Reality) Center of Excellence (COE) addresses the challenges of protecting the wide range of soft targets and crowded places (STCPs) in our homeland. The scope of these challenges is vast: there are hundreds of thousands of STCPs in the U.S., accessed by tens of millions of people each day. Because of the volume and variability of STCPs, there are frequently limited security or protective measures and limited resources to enhance those measures. Three recent changes that have augmented these challenges are: 1) a more diverse set of actors and motivations, 2) communication advances that have compressed the timeline to detect and prevent violence, and 3) greater access to a range of weapons. Compounding these technical challenges, STCPs frequently straddle the public-private domain, and there are insufficient numbers of Homeland Security professionals with the training needed to address these challenges as they presently exist and will evolve over time.

The **SENTRY vision** (**Figure 1-1**) to address these challenges is a suite of systems called the Virtual Sentry (VS). Versatile, scalable and cost-effective, the VS will function semi-autonomously with the capability to rapidly integrate and process data to provide real-time decision support to STCP decisionmakers (e.g., school principals or the heads of surface transportation facilities) as they interact with first responders to detect, deter and mitigate targeted violence. In support of this vision, the **SENTRY mission** is two-fold: (1) conduct **stakeholder-informed research** to advance knowledge to **transition to industry** for development of VS technology for use by STCP stakeholders at every scale, both public and private, and (2) educate both the current and next generations of the homeland security **workforce** in STCP technology, using VS as a motivator.



VISION: VIRTUAL SENTRY

Real Time Decision Support System for STCP Stakeholders

- Enables situational awareness of STCP targeted violence
- Versatile, scalable and cost-effective
- Open-source secure data fusion from multimodal data
- Semi-autonomous and real-time

VIRTUAL SENTRY ENABLED BY INTEGRATED STRATEGY FOR ★ RESEARCH ★ TRANSITION ★ WORKFORCE DEVELOPMENT

- Partnership-based to extend reach of COE
- Informed by industrial and policy advisory boards, interactions with DHS components
- Combines strengths of three emeritus COEs

Figure 1-1*. Integrated SENTRY strategy for research, transition and workforce development, anchored by the Virtual Sentry vision. Open source enables external and in-kind contributions.*

A. Partners

The SENTRY team combines the strengths of three emeritus DHS COEs: ALERT (Awareness and Localization of Explosives-Related Threats), CCICADA (Command, Control, and Interoperability Center for Advanced Data Analytics) and CREATE (Center for Risk and Economic Analysis of Threats and Emergencies). ALERT, led by Northeastern University (NU), brings a strong track record of threat anomaly detection using advanced sensor technologies and signature analysis algorithms. CCICADA, led by Rutgers University (U.), has pioneered in the protection of STCPs such as stadiums and the surface transportation infrastructure. CREATE, led by the U. of Southern California (USC), has developed optimal methods of assessing risks due to unanticipated attacks on soft target venues. All three emeritus COEs have achieved meaningful transition to the field with significant impacts on workforce development and first responder training. Other SENTRY academic partners include Boston U. (BU), U. Florida, Rensselaer Polytechnic Institute (RPI), Tufts U., U. of Notre Dame (ND), U. of Puerto Rico-Mayaguez (UPRM, **a Minority-Serving Institution**), U. of Rhode Island (URI), and the State U. of New York-Buffalo (UB).

SENTRY has established partnerships well beyond academia as well, to both inform and transition SENTRY research and workforce development elements to stakeholder end-users: industry, national laboratories, operators of both public and private STCPs, and state and local governments. To that end, SENTRY has established industrial and policy-practitioner advisory boards comprised of experts from the public and private security sectors. These bodies help facilitate interactions with DHS components, visits to STCPs, and help structure SENTRY convening events like the highly successful ALERT ADSA workshops. SENTRY leadership will pursue a continuous process of stakeholder need identification and response to address protection of STCPs.

B. Research Program and Testbeds

Figure 1-2 outlines the **SENTRY research program** and outlines the detailed organization, research and facilities needed to achieve the ten-year VS vision. **Level 3** shows the grand challenges that must be addressed to protect all STCPs. An analysis of the barriers associated with these grand challenges leads to the fundamental research program at **Level 1**. The research area entitled “Real Time Management of Threat Detection & Mitigation (RA)” is the heart of the VS design orchestrating the real-time data management and decision support that will enable effective protection of the STCP venues. The other research areas at Level 1 (RB, RC and RD) support RA in the development of advanced sensing strategies, risk assessment and architectural designs.

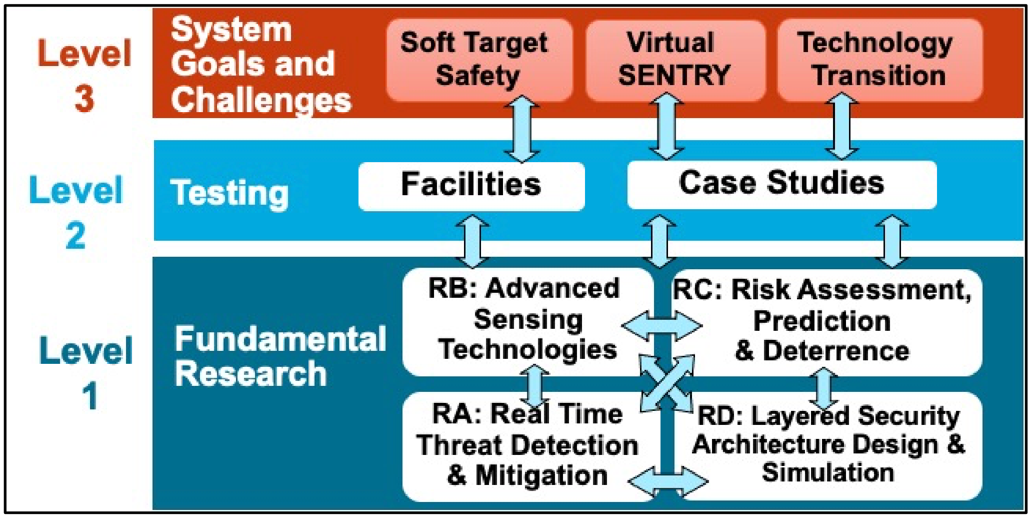

Level 3
System Goals and Challenges
Soft Target Safety
Virtual SENTRY
Technology Transition
Level 2
Testing
Facilities
Case Studies
Level 1
Fundamental Research
RB: Advanced Sensing Technologies
RC: Risk Assessment, Prediction & Deterrence
RA: Real Time Threat Detection & Mitigation
RD: Layered Security Architecture Design & Simulation

***Figure 1-2**. The SENTRY research structure ties STCP technical challenges (Level 3) to fundamental research (Level 1) and identifies the facilities and case studies needed (Level 2) to test outcomes from Level 1 at scale before integrating them into the overall VS concept.*

Ten projects have been identified for the Year 1 SENTRY research program. These projects will develop novel solutions for the foundational, enabling elements of a VS, such as: development of new sensor concepts; application of artificial intelligence (AI)/machine learning (ML) to risk assessment; quantitative threat deterrence; development of layered security architectures; and providing methods for fusing data and other information. More details on these projects are given in Section 2 and Appendix A.

Existing unique testbed facilities indicated in **Level 2** will enable testing and evaluation of Level 1 research outcomes for continuous improvement of the overall VS system over the ten-year period of the COE. Use of these facilities will augment the research in several ways. For example, The Colosseum and Agile Communications Facility (TB) will enable the incorporation of 5G/6G strategies to assess the robustness of first responder interoperability during a disaster, and the Guardian Centers Realistic Rail Infrastructure training facility (TD) will enable testing with realistic attack and defense scenarios. In addition to the test facilities, SENTRY created a strategy to embark on several case studies focused on specific STCP venues that will enable the various stages of the VS design and implementation to be tested. The first case study, defined in Year 1, focuses on K-12 school safety. This will be followed in Year 2 by a case study focused on securing surface transportation. Future cases studies will explore other STCP venues such as large stadiums and shopping malls. The connections and results engendered by the testing at Level 2 will provide a pathway to transition for public and private development of the VS components. More details on these facilities and case studies are given in Section 2.

C. Workforce and Professional Development Program

The SENTRY **workforce and professional development program (WPDP)** has identified five unique projects that are integrated with the research vision and developed with the intention of building networks among DHS Stakeholders to enhance the educational, training, and research experiences of the current and future Homeland Security Enterprise (HSE) workforce. These stakeholders include COE students and researchers, HSE and DHS professionals, and relevant industry, government and community members. To engage the SENTRY graduate and undergraduate students with HSE practitioners, we have developed projects that will encourage and facilitate interaction through a) challenging hackathon competitions developed collaboratively with HSE component leadership and b) continual development of meaningful internship, co-op and research experiences at the SENTRY academic labs and testbeds, HSE and DHS operational areas, and relevant public and private entities. More details on the WPDP components are given in Section 3.

Guided by a seasoned leadership team with support from experienced administrative staff, SENTRY will effectively and professionally promote all COE activities across the HSE. Leadership will also formally evaluate this research-education strategy and program annually to adjust or replace existing efforts with new projects to better address the VS vision and needs of the DHS, with additional evaluation via the DHS biennial review process.

D. Transition Program

The **SENTRY transition strategy** includes regular stage-gate-guided, metric-based project evaluations, yearly stakeholder driven SWOT analyses, market and competitive landscape analyses, and project-transition partner matchmaking. Identifying and collaborating with the right industrial partners and DHS components is key. Engaging these stakeholders throughout the stage-gate research and development (R&D) process will allow SENTRY to adapt and respond to the ever-evolving HS landscape. An important aspect of this pathway is the collaboration with industrial partners and National Labs that can provide resources to help enable the open-source VS platform. The SENTRY transition efforts are described in detail in Section 4.

E. Industrial Liaison Initiatives and Partnerships

SENTRY benefited from the prior collaborative links forged by ALERT and by Northeastern's National Science Foundation (NSF)-funded Engineering Research Center, Gordon-CenSSIS, with industry, practitioners and government organizations. Many of these partners continue to engage with SENTRY through membership fees and through participation in SENTRY events. IAB members provide the center with opportunities for researchers and students to work at their facilities, as well as access to research and development (R&D) leaders, real system-level applications, state-of-the-art hardware and software, willing partners for technology transfer, and team members for proposals for additional funding and sustainability. Conversely, SENTRY will provide its collaborators with access to talented professors, postdocs, graduate students, undergraduate students, and innovative research. Together, the industrial/practitioner, government, and academic collaboration has been – and will continue to be – a powerful vehicle for advanced development. The COE's industrial/practitioner and government partnerships are discussed in more detail in Section 5.

F. Strategic Workshops and Events

SENTRY Workshops are a key element of its ability to adapt its research program over the 10-year timeframe of the Center. Indeed, part of the Center of Excellence (COE) mandate from DHS is to develop, implement and disseminate its strategy to enable the achievement of the Center's grand challenges. To support this effort, SENTRY will continue to host an ALERT-initiated workshop series known as **Advanced Developments for Security Applications (ADSA)**. The outcomes of each workshop are documented in a report that articulates a roadmap recommending prioritized areas of long-range fundamental research. An initial SENTRY-oriented ADSA workshop was held on May 3-4, 2022, supplementing the 24 held previously under ALERT. The theme of this workshop was Protecting Surface Transportation and Other Soft Targets. In addition to the ADSA workshops, a brainstorming session on the school safety case study was held in April 2022 followed by a Futures Workshop on July 19 and 21, 2022 facilitated by PNNL. The SENTRY workshop activities are discussed in more detail in Section 6.

G. Management and Evaluation

The **Policy-Practitioner Advisory Board (PAB) and Industrial Advisory Board (IAB)** guide SENTRY activities from complementary perspectives. Members of the PAB include world-class experts in the specific venues and challenges of STCPs and IAB representatives from leading commercial firms will help provide technology guidance toward the development of the VS. Both PAB and IAB members will participate in SENTRY events as appropriate. The IAB is comprised of industrial organizations who have committed participation in the center through membership fees or in-kind support. The SENTRY Industrial Liaison maintains continuous connection with this important group. More details on the PAB and IAB are provided in Section 7.

The **SENTRY leadership and management team** includes experienced personnel with proven records of accomplishment. This team is an extension of the ALERT leadership, augmented by the SENTRY research and WPDP leaders. The SENTRY leadership and management team is discussed in more detail in Section 7.

H. Budgetary Information

The SENTRY Year 1 **budget information**, categorized by both object class and project, is discussed in Section 8 and reported in Appendix A and B.

I. Data Acquisition & Management Plan, Information Protection Plan, and Research Safety Plan

As required by the COE Cooperative Agreement, SENTRY has developed a **Data Acquisition & Management Plan**, **Information Protection Plan,** and **Research Safety Plan**. These plans are discussed in more detail in Section 9 and Appendix C.

J. Summary

This annual report provides a broad overview of the strategic plan, goals, and deliverables for the SENTRY Center of Excellence. The SENTRY leadership has a firm base from which to quickly adapt to new research and education priorities related to the daunting mission of protecting STCPs. Before turning to the detailed description of the SENTRY program, we first present a brief description of several Year 1 highlights.

1.2 SENTRY YEAR 1 HIGHLIGHTS

A. SENTRY Director Appointed Co-PI of NSF INCLUDES Alliance

SENTRY Director and Northeastern University distinguished professor of electrical and computer engineering, Michael Silevitch, serves as co-PI of the Engineering PLUS (Partnerships Launching Underrepresented Students) National Science Foundation (NSF) INCLUDES (Inclusion Across the Nation of Communities of Learners of Underrepresented Discoverers in Engineering and Science) Alliance, a 5-year $10M grant awarded August 2021. Engineering PLUS seeks to achieve tranformative, systemic and sustainable change that will incrase the annual growth rate in the nu mber of Black, Indigenous and People of Color (BIPOC) and women obtaining engineering degrees. By driving the growth of engineering undergraduate degrees by 10% and graduate degress by 5% across these underrepresented populations, Engineering PLUS aims to increase the annual number of degrees awarded BIPOC and women to 100K undergradaute degrees and 30K graduate degr ees by 2026, and to establish a future growth rate to bring the number of women and BIPOC engineers much closer to partiy with their percentage of the U.S. population by fostering system changes at key transition points of the engineering education pathway. Engineering PLUS will link to and strongly support SENTRY's WPDP and diversity, equity and inclusion efforts.

Figure 1-3: *Engineering PLUS NSF INCLUDES Alliance Leadership Team and other key personnel at the Engineering PLUS Design Lab at Northeastern University on May 11, 2022. Michael Silevitch, SENTRY Director, serves as a co-PI for Engineering PLUS.*

B. SENTRY School Security Case Study Brainstorming Session and Futures Workshop

On April 12, 2022, SENTRY hosted a School Security Brainstorming Session, held virtually via Zoom, for the purpose of facilitating open discussion between SENTRY researchers and personnel, PAB members, and five school security stakeholders on how a Virtual Sentry (VS) could best address safety concerns on K-12 school venues. Points of discussion included: deterrence, countermeasures, locations of primary concern, current best practices, privacy concerns, architectural issues, and use of CCTV cameras in schools. SENTRY summarized the key takeaways from the session in an internal report that will be utilized to inform

SENTRY's continued work regarding school security. The session also established connections with key school stakeholders that we plan to develop into partnerships in assessing the utility of the VS system.

Building on the information gathered from the School Security Brainstorming Session, in Year 2, SENTRY hosted a Future of School Security Meeting in collaboration with Pacific Northwest National Laboratories (PNNL) on July 19 and 21, held virtually via Zoom. The meeting was an invitation-only moderated collaboration to ensure an open exchange of ideas on the art of the possible with respect to the future of school security. Participants were specifically selected based on their experience and expertise, with stakeholder representation from SENTRY researchers, first responders, school security personnel, teachers, school administrators, phycologists/social workers, technologists, DHS components, parents, and students. PNNL will collate the feedback gathered at the Futures meeting into a final report and detail recommendations on technologies, requirements and priorities of a VS framework in the school security space. SENTRY will incorporate the findings from this report as we continue work on the school security case study, including identifying specific venues to assess the utility of the VS system.

C. SENTRY Hosts ADSA25

SENTRY hosted the 25th ALERT-initiated Advanced Developments for Security Applications (ADSA25) workshop on May 3-4, 2022, which addressed the theme "Protecting Surface Transportation and Other Soft Targets." This hybrid event was hosted at Northeastern University in Boston, Massachusetts, as well as virtually on Zoom, allowing participants from academia, industry and government to gather in-person for the first time since the onset of the COVID-19 pandemic while maintaining an option for remote participation. During the two-day workshop, 160 participants convened with subject matter experts and leaders to discuss detecting people with malicious intent and their weapons, hardneing venues, rapid response to events, system integrity, transparency and bias in AI/ML algorithms, emerging technologies, protection case studies, and other related topics. As noted by attendees, event highlights included the hybrid format, which allowed particiapnts and high-quality speakers to gather from all over the world, engaging discussion across a variety of topics, and the opportunity to connect with other security stakeholders.

Figure 1-4*: Sonya Proctor, Assistant Administrator for Surface Operations, TSA, presenting at ADSA25.*

Section 2: Research Program and Testbeds

2.1 THE FOUR SENTRY FUNDAMENTAL RESEARCH THRUSTS

SENTRY's comprehensive research approach, outlined in **Figure 2-1**, allows for continuous feedback between research outcomes and stakeholder needs and a pathway to transition for public and private development of the Virtual Sentry (VS) components. The goal of the SENTRY fundamental research program is to develop foundational results that can improve our ability to protect soft targets and crowded places (STCPs) at different levels. Proposed projects, organized into four research thrusts (RA-RD, shown on **Figure 2-1**), approach this goal **with techniques that work at multiple time scales**, from design concepts for STCPs, to real-time information extraction and decision support systems for networks of advanced sensor concepts. In this subsection, we first provide an overview of and relationship between the four thrusts and associated ten research projects we have selected for the first two years of the proposed Center, as well as their contribution to the SENTRY VS vision. Thrusts are presented in reverse order, from slowest to fastest time scale.

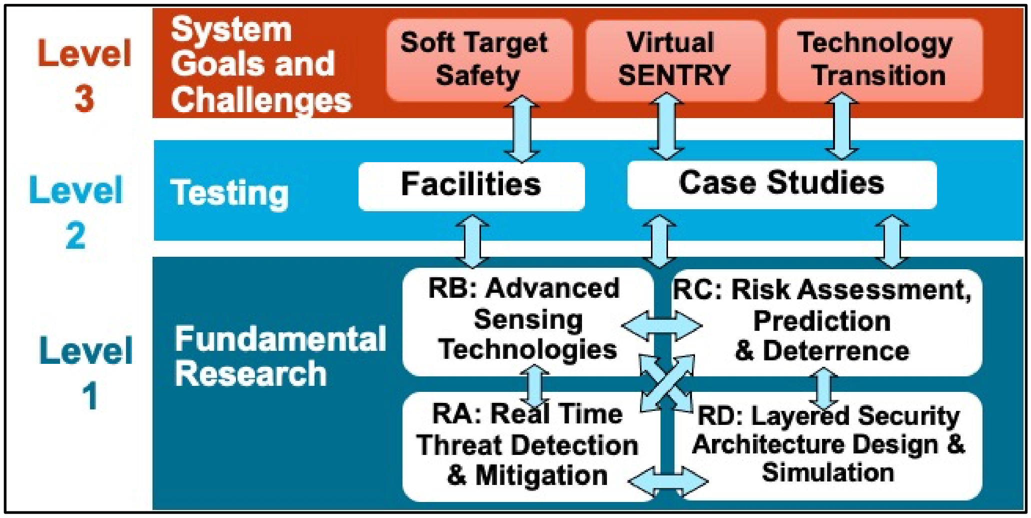

Level 3
System Goals and Challenges
Soft Target Safety
Virtual SENTRY
Technology Transition
Level 2
Testing
Facilities
Case Studies
Level 1
Fundamental Research
RB: Advanced Sensing Technologies
RC: Risk Assessment, Prediction & Deterrence
RA: Real Time Threat Detection & Mitigation
RD: Layered Security Architecture Design & Simulation

Figure 2-1. *The SENTRY research structure ties STCP technical challenges (Level 3) to fundamental research (Level 1) and identifies the facilities and case studies needed (Level 2) to test outcomes from Level 1 at scale before integrating them into the overall VS concept.*

Research Thrust D (RD): Layered Security Architectural Design and Simulation (Lead: Michelle Laboy, Northeastern University)

At the slowest scale, Project **RD.1:** Architectural Design Research: Integrating Security in the Public Realm seeks to develop principles and techniques to design venues and environments that enhance the ability to protect against diverse attacks. The project will generate principles and protocols for design that enhance passive security features and enable augmentation with active surveillance and mitigation capabilities as developed by other SENTRY projects. A complementary effort is Project **RD.2:** Dynamic Digital Twins for Secure and Smart Civic Space. This project aims to improve existing venues through architectural modifications and installation of new security features. It proposes to capture accurate computer models of existing venues and use simulations coupled with mathematical optimization techniques to identify desired modifications and enhancements. These simulations can also support the design research of Project RD.1 and can be used in exercises to support venue operators in exploring alternative scenarios. Crowd members are a critical component of STCPs; Project **RD.3:** Real-Time Crowd and Attacker Forecasting for Risk Assessment and Threat Mitigation proposes to develop models that enable the ability to forecast crowd behavior in response to a broad range of attacks and mitigation activities. Crowd behavior is influenced strongly by architectural design, so this provides needed support to Projects RD.1 for evaluating the impacts of alternative design principles, and RD.2 for accurately representing crowd behavior in the models.

Research Thrust C (RC): Threat Risk Assessment, Prediction and Deterrence (Lead: Jun Zhuang, University at Buffalo)

This thrust works at a faster time scale, in which the architecture of the venues is already established, but we want to assess risks to those venues. Project **RC.1** seeks to develop AI tools for data mining of social media, geospatial data platforms, and other sources of information to extract insights on potential threats and thus assist strategic and tactical security risk planning. The work will focus on explainable ML algorithms that will make the decisions accessible to users. The project will address issues such as how to generalize the small amount of training data relevant to the sparse attacks on previous STCPs. Project **RC.2**: Protecting Soft Targets (ProSoT): A Game-theoretic Framework for Multi-target, Multi-layer Defense against Strategic Attackers, is a complementary effort. It focuses on the problem of allocating resources to defend multiple potential STCPs, assuming that an intelligent enemy will be able to select STCPs that are easiest to attack and have the most negative impact. This work will offer insights and tools that can guide risk-informed security planning and security system design, particularly when venues can have multiple security layers.

Research Thrust B (RB): Advanced Sensing Technologies for Threat Awareness (Lead: Carey Rappaport, Northeastern University)

This thrust develops new sensing capabilities to detect threats. Current sensors such as metal detector portals and chemical sniffers require close-in inspection; the goals of these two projects are to develop new stand-off sensor concepts for detecting concealed threats in crowds. Project **RB.1:** Multi-Sensor threat assessment platforms is concerned with chemical and biological threats to STCPs. The project proposes to develop vapor sensors that can detect and localize vapor plumes emitted by chemical and biological agents. The project extends concepts proposed for short distance sensing so that they can be used in crowds and larger spaces. The proposed sensing systems would be inexpensive to deploy and operate, so that they could be integrated in multi-modal sensor networks. Project **RB.2**: Stationary and Aerial based RF/Radar Detection of Drones, Concealed Threats and Anomalous Communications Signatures is concerned with detection of concealed states such as weapons and explosives, as well as threats from unmanned air vehicles. The goal of this project is to design networks of inexpensive millimeter (mm) wave radar arrays and RF receivers. Distributed mm wave radar arrays provide signatures to detect concealed weapons and explosives. Similarly, passive monitoring of RF emission patterns can provide indicators of deviations from normal patterns, identifying areas for further investigation.

Research Thrust A (RA): Real Time Management of Threat Detection & Mitigation (Lead: David Castañón, Boston University)

This thrust supports the protection of STCPs in real time operations. Project **RA.3**: Real time Video Surveillance for Threat Detection and Mitigation will develop new methods to extract threat information from real-time networks of video cameras which are ubiquitous sensors in many STCPs. This project will develop algorithms to (1) detect anomalous events in crowds, based on learning models of normal patterns from observations, (2) to track suspicious individuals across networks of cameras, exploiting the pan-tilt-zoom capabilities of such cameras and (3) for the classification of individual actions and behaviors to detect anomalies and threats, with an emphasis on algorithms that are fair, unbiased, trustworthy, and explainable.

Project **RA.2**: Low Complexity AI Based Fusion of Crowd-Sourced Heterogeneous Data Streams for Real-Time Threat Detection and Mitigation is focused on exploiting real-time information from personal devices such as cell phones. It seeks to develop models and algorithms to process data from a collection of crowd-sourced mobile sensors to detect and monitor emerging threats and to prompt device owners for additional data when desired. An important aspect of this work is to develop low-dimensional representations of the extensive data provided by crowd-sourced sensors so that anomalous data patterns can be identified. Project **RA.1**: Real-time Management of Adaptive Surveillance and Mitigation seeks to develop decision support systems that assist decision makers in deployment and real-time control of layered surveillance systems and threat mitigation activities for STCPs. These decision support systems exploit the results of many SENTRY projects: architectural features of the venue as designed by **RD.1** and enhanced by **RD.2**, potential threats identified by **RC.1**, novel sensing capabilities from **RB.1** and **RB.2**, and information extraction from video sensors **RA.3** and crowd-source sensors **RA.2**. The decision support systems fuse the diverse sources of information, recommend tasking of additional sensors to localize and confirm potential threats, and evaluate alternative courses of action to mitigate the identified threats, to support the decision makers in selecting appropriate mitigation.

Details on each research project – including milestones, performance metrics, integration with the VS framework, stakeholder and end-user engagements, project risk register, and budget information – can be found in Appendix A.

2.2 SENTRY TESTBED FACILITIES

Level 2 of Figure 2-1 is a testing level. It contains both facilities for the testing of new technologies as well as case studies which are testbeds based at specific venues that will pilot the development of the Virtual Sentry (VS). This subsection presents an overview of the SENTRY Testbed Facilities.

Testbed TA: NU ECUAS Lab Drone Offense & Defense Facility

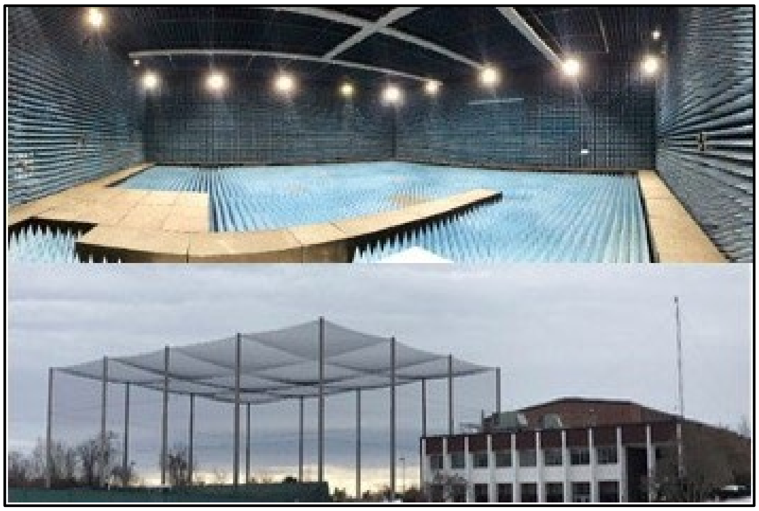


***Figure 2-2**: ECUAS will enable the collection of drone-related data to refine VS decision support algorithms.*

The Northeastern University (NU) Expeditionary Cyber and Unnamed Aerial System (ECUAS) is a one-of-a-kind facility that enables drone technology discovery and innovation including flight systems and vehicles, communications, sensing, positioning, navigation and timing. It consists of both indoor and outdoor test ranges (shown in **Figure 2-2**) for testing aerial and ground systems. Tools integrated into the 50'x50'x22' anechoic chamber are: 1) Arsenal of drones and multi-modal sensor systems; 2) State of the art software defined radios and up to 64 antenna arrays to transmit/receive arbitrary waveforms for jamming, communications and control; 3) Navigation testing (with interference) using a Global Navigation Satellite System Simulator; 4) Cyber security testing of wireless devices for vulnerability/exploitation analysis; and 5) 24 Camera 360° optical tracking system for precise indoor positioning. The outdoor range is a 200'x150'x60' netted enclosure for dedicated UAV testing that does not require any Federal Aviation Administration authorizations for flight activities. A netted flight corridor provides seamless transition between indoor and outdoor areas. ECUAS is available for use with support staff, for a fee. A short video on ECUAS and its capabilities can be viewed online: www.youtube.com/watch?v=-6fTr5y80xk.

ECUAS will serve as an environment where structured test scenarios can be configured that integrate drones, distribute multi-modal sensors, simulate data feeds from public sources, and utilize real-time data processing using machine learning (ML)/artificial intelligence (AI). Its arsenal of drones and sensor system will enable algorithms for real-time data fusion and decision support to be assessed and integrated with the advanced detection sensors. In this sense, it provides the ecosystem through which VS subcomponents can be integrated and tested together. For example, use of drones with integrated sensors for real-time data collection is a key subcomponent of the proposed VS. Testing real-time data collection and ML/AI-based analytics will require a location that can integrate sensor feeds from drones and ground sensors with a communications network and high-performance computing back-end – all of which are available at ECUAS. With trained pilot and engineering staff, ECUAS will aid in the design and execution of tests that require drone swarms with multi-modal sensing capabilities that leverage the indoor and outdoor environments. Additionally, enhanced testing and analysis techniques, such as the use of Augmented Reality (AR), in conjunction with live sensor feeds can be explored through ECUAS. In one scenario, a simulated crowd with threats injected via AR into sensor feeds can greatly benefit live scenario exercises that are used to assess technologies, methods, training and preparedness for specific malicious events. Injection of threats via AR into sensor feeds will allow for robust testing of automated decision making and command/control systems as well as situational awareness information passed to first responders.

Testbed TB: NU Colosseum 5G/6G Agile Communications Facility

Colosseum, housed within NU's Institute for the Wireless Internet of Things (IoT), led by Prof. Tommaso Melodia, is the world's largest network emulator with hardware in the loop. Originally developed by the Defense Advanced Research Projects Agency (DARPA) to support the Collaborative Spectrum Challenge (SC2) through an investment of $20M+, Colosseum is a data center with 256 software-defined radios emulating in real-time the 65,536 channels generated between all the radios and their evolution in time. Colosseum enables creation of virtual complex wireless environments and emulates wireless signals traveling through space and reflecting off multiple objects between transmitters and receivers. With Colosseum, any realistic network scenario (with effects like multipath, fading, occlusions) can be created. Colosseum can create virtual worlds with sophisticated 5G and IoT wireless systems, as if the radios were operating in an STCP such as a downtown area or shopping mall. For the first time, researchers are able to conduct fully controlled and reproducible radio-channel experiments at scale with technologies that will be the foundation of 5G and the wireless IoT, spectrum sharing, smart cities, connected vehicles, and industry 4.0, among others.

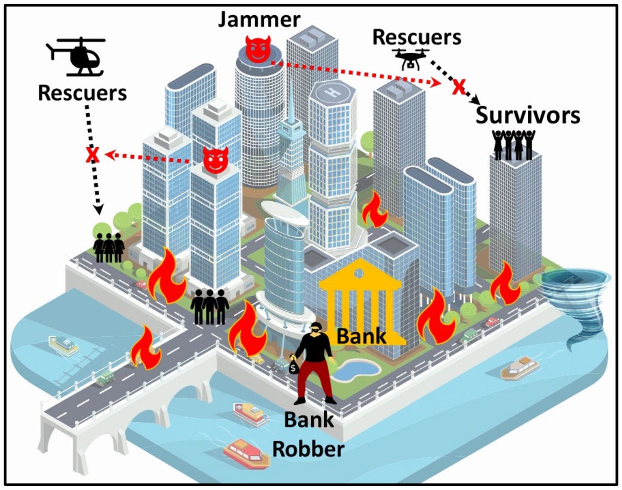


Figure 2-3*: Depiction of an STCP attack and how Colosseum enables optimizing communications channels.*

Figure 2-3 depicts an example of an STCP attack situation to be emulated: multiple explosions happening simultaneously throughout a city destroying most of the existing communication infrastructure (e.g., cellular towers). First responders and local authorities dispatch vehicles – both unmanned (e.g., drones) and manned (e.g., helicopters) – to search for and rescue survivors, e.g., using alternative technologies to form ad hoc infrastructure-less networks with them. However, multiple adversaries maliciously act to jam first responder communications to hinder their rescue operations. At the same time, bank robbers – who are complicit with the malicious adversaries – are leveraging this diversion to go unnoticed. In Colosseum, this scenario can be emulated to effectively test technologies and solutions not only to rescue survivors, but also to locate and eliminate threats to public safety (i.e., jammers and bank robbers in the provided example). At first, the urban environment could be modeled with ray tracing software of electromagnetic field solvers. Then, the failure of the existing infrastructure can be emulated by disrupting any form of ongoing signal and communication. Survivors seeking a safe place to wait for rescuers can be emulated through random group mobility, which would possibly involve wireless channels with multiple diffractions and scattering. First responder vehicles, instead, can be emulated through multiple nodes wandering at different speeds and altitudes (e.g., in the case of drones and helicopters) with an air-to-ground channel with ground nodes (i.e., survivors). A similar channel would be leveraged to consider jammers. Finally, bank robbers, who are aware in advance of the upcoming disaster, would be equipped with low-power local-area technologies to coordinate with each other while robbing the bank, thus requiring the emulation of an indoor wireless channel mostly isolated from the outdoor environment.

To provide an example of Colosseum emulation capabilities, **Figure 2-4** shows an emulated RF scenario corresponding to the realistic urban deployment of downtown Rome, Italy (next to the actual Roman amphitheater). In this case, Colosseum was used to instantiate an AI-driven softwarized 5G network. Specifically, this emulation is done through so called RF scenarios designed to capture and reproduce the channel conditions of a variety of real environments (e.g., mall, desert, rural and urban settlements, contested adversarial environments, etc.). This emulation involves processing the radio signals generated by the users in real-time through FPGA-based Finite Impulse Response (FIR) filters, which apply pre-computed filter taps of the specific emulated scenario.

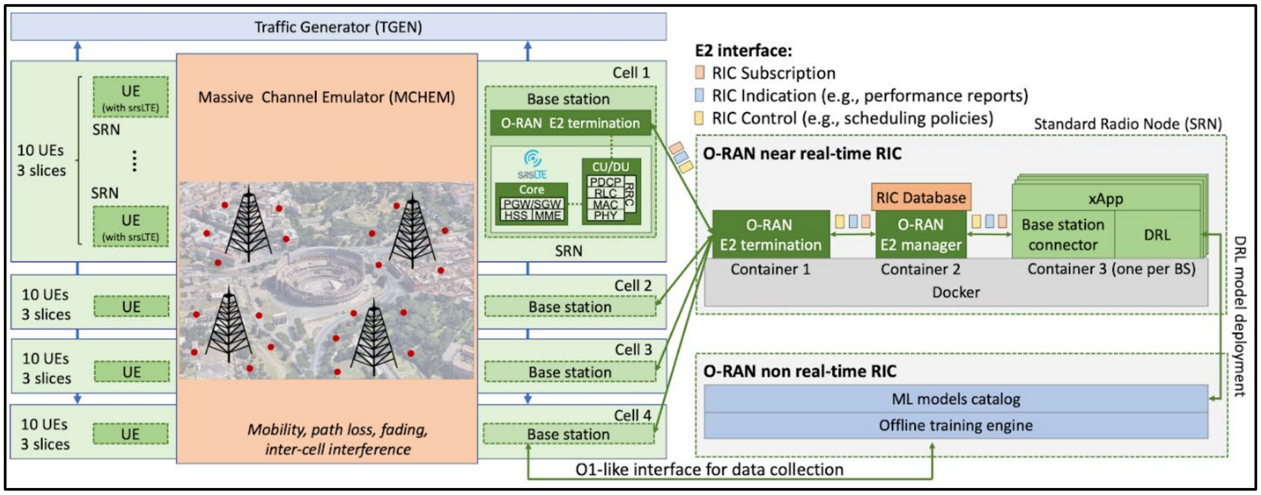


***Figure 2-4**: Realistic emulation of urban scenario with AI-enabled softwarized 5G network on Colosseum.*

Testbed TC: Rutgers Living Lab Public Venues with Digital Twin

Rutgers' Living Labs provide access to campus spaces to observe buildings and people. These include a large football stadium, a smaller soccer stadium, basketball arenas, hospital facilities, dining halls, dormitories, and other contextually relevant environments (see **Figure 2-5**). Its use in SENTRY and the associated digital twin capability are discussed in Section 2.1 in the RD.2 and RD.3 projects.

Figure 2-5: *Left: "Living Lab" Venues include dining halls and other STCP-relevant environments. Right: Rutgers campus includes numerous living lab environments (red dots).*

Testbed TD: Guardian Centers Realistic Rail, Infrastructure Training Facility

Guardian Centers, LLC (GC) is a disaster preparedness and tactical training center that provides custom services, including complete exercise design and planning, training and certification, and full-service logistics support. As indicated in their letter of support, the GC campus can simulate real attack scenarios around soft target venues such as light rail, schools and large structures. The attack scenarios can be used to help train first responders as well as provide datasets to help enable the VS decision support algorithms. **Figure 2-6** shows some of GC's capabilities.

Figure 2-6*: The Guardian Centers facility will enable realistic data collection and first responder training.*

2.3 SENTRY CASE STUDIES

SENTRY has launched a series of case studies to assess the transition of its research into specific stakeholder venues. The ultimate intent of these case studies is to develop a pragmatic understanding of the needs associated with specific STCP venues and how those needs translate into an implementation of the VS system. In Year 1, SENTRY focused on the following case studies: School Security and Secure Surface Transportation. To date, the preparation for these case studies is as follows:

School Security

The School Security case study is being driven by the expertise inherent in the SENTRY Policy-Practitioner Advisory Board (PAB) – namely Jacob Ludes, Former President/CEO of the New England Association of

Schools and Colleges, who has extensive experience with and knowledge of school security needs and best practices that qualify him to guide this effort. In Year 1, SENTRY took the following steps regarding the school safety case study:

A. SENTRY School Security Case Study Working Group

An initial working group of 20 SENTRY personnel assembled February 2022 to address the school security case study, meeting bi-weekly to discuss the problem statement and define the next steps SENTRY should take in order to successfully implement the VS system in school venues.

B. SENTRY School Security Brainstorming Session

On April 12, 2022, SENTRY hosted a 3-hour School Security Brainstorming Session, held virtually via Zoom, for the purpose of facilitating open discussion between SENTRY personnel and five school security stakeholders on how a Virtual Sentry could best address safety concerns for K-12 school venues. The invited school security panelists included:

- Dr. George Edwards, Director of Accreditation, New England Association of Schools and Colleges
- Dr. Joseph Erardi, Superintendent (retired), Newtown, Connecticut, Public Schools
- Dr. Penelope (Penny) Eucker, Executive Director, STEM School, Highlands Ranch, CO
- Dr. Lawrence Filippelli, Superintendent, Lincoln Public Schools, Lincoln, RI; President/Proprietor, The Education Consortium
- Dr. Kevin McCaskill, Senior Administrator Secondary Schools, Boston, Massachusetts, Public Schools

The following points of discussion were distributed to participants in advance of the meeting to guide the conversation:

- School/campus areas or locations of concern
- Privacy issues which imposed limitations on security actions or installations
- Countermeasures/detection capabilities installed or desired
- Architectural impacts/solutions for new designs or retrofitted in schools
- Deterrence; is it a meaningful factor, and how is it accomplished?
- What are the best practices/drills to prepare for threats or such incidents?
- How can CCTV and classroom televisions be used for school security?

SENTRY personnel summarized the key takeaways from the session in an internal report that will be utilized to inform SENTRY's continued work regarding the school security case study. The session also established connections with key school stakeholders that SENTRY plans to develop into partnerships in assessing the utility of the VS system.

C. Future of School Security Working Meeting

Building on the information gathered from the School Security Brainstorming Session, in Year 2, SENTRY hosted a Future of School Security Meeting in collaboration with Pacific Northwest National Laboratories (PNNL). The meeting was an invitation-only moderated collaboration which allowed for an open exchange of ideas on the art of the possible with respect to the future of school security. 37 external participants were specifically selected based on their experience and expertise, with stakeholder representation from SENTRY researchers, first responders, school security personnel, teachers, school administrators, phycologists/social workers, technologists, DHS components, parents, and students. Year 1 funding of $45K was allocated to support this ideation event, which took place virtually in two 4-hour sessions on July 19 and 21, 2022.

PNNL is in the process of collating the feedback gathered at this Futures meeting into a final report which will provide recommendations on technologies, requirements and priorities of a VS framework in the school security space. SENTRY will incorporate the findings from this report as we continue work on the school security case study.

In Year 2, specific venues will be identified to assess the utility of the VS system approach. Funding will be allocated from the $1M Year 2 SENTRY Plus-up funds to support this effort and that of the case studies in general.

Secure Surface Transportation

The Secure Surface Transportation case study is being driven by the prior work that Prof. Jie Gong and the Rutgers CICCADA COE have done in collaboration with the New Jersey Transit Authority. Specific steps for the SENTRY research team to learn about the problem in Year 1 included the following:

A. Meeting with the New Jersey Transit Authority

   On May 9, 2022, a meeting took place between SENTRY personnel and the New Jersey Transit Authority to discuss the development of a collaboration to enhance the resilience of the facility to withstand both man-made as well as natural threats. The outcome was an agreement to work together toward understanding of their problems and the creation of a meaningful VS framework. Jie Gong and Fred Roberts from Rutgers and CICCADA, along with George Naccara and other members of the PAB, will lead the effort.

B. Meeting with TSA Stakeholders

   George Naccara initiated conversations with Sonya Proctor, Assistant Administrator for Surface Operations, Transportation Security Administration (TSA) and other TSA personnel to discuss the Secure Surface Transportation case study and the Rutgers/New Jersey Transit project and possible SENTRY/TSA collaboration. Both parties agreed that SENTRY should utilize existing TSA surface transportation testbeds as initial venues, with Hoboken/New Jersey Transit Terminal as one of those testbeds. SENTRY plans to initiate similar conversations with Cybersecurity and Infrastructure Security Agency (CISA) stakeholders to explore other possible collaborations.

C. Secure Surface Transportation Brainstorming Session

   SENTRY is planning a brainstorming session for fall 2022 to explore the Secure Surface Transportation case study. The format of this session will be similar to the School Security Brainstorming Session that took place in spring of 2022. Proposed participants include representatives from the following:

   - Los Angeles County Metropolitan Transportation Authority
   - Massachusetts Bay Transit Authority

- New Jersey Transit
- New Orleans Regional Transit Authority
- Washington Metro

SENTRY plans to initially focus on the Hoboken/New Jersey Transit Terminal to examine the compounding of threats from man-made attacks and natural hazards. The effort will create a strategy to link with the other existing TSA Requirements and Capability Analysis (RCA) transportation testbeds that are part of a national surface security technology field testing partnership.

In Year 2, SENTRY will identify specific venues to assess the utility of the VS system approach. Funding will be allocated from the $1Million Year 2 SENTRY Plus-up funds to support this effort and that of the case studies in general.

2.4 CONCLUSION

SENTRY maintains a strategic research approach that supports the feedback between research outcomes and stakeholder needs, which will ultimately lead to transition pathways for public and private development of the Virtual Sentry (see Figure 2-1). In Year 1, SENTRY made significant progress with the School Security case study and will continue with that while commencing efforts to explore the Secure Surface Transportation case study in Year 2, which in turn will continue to inform the effort of the four research thrusts. Ultimately, our work will result in the pragmatic transition of SENTRY-developed technologies that DHS will be able to incorporate into requirements for future systems to help safeguard our nation's soft targets and crowded places.

This page intentionally left blank.

Section 3: Workforce and Professional Development Program

3.1 INTRODUCTION AND OVERVIEW

The SENTRY Workforce and Professional Development Program (WPDP) includes unique projects that were developed with the intention of building networks among DHS stakeholders to enhance the educational, training, and research experiences of the current and future DHS workforce. These stakeholders include COE students and researchers, HSE and DHS professionals, and relevant industry, government and community members. To engage the SENTRY graduate and undergraduate students with HSE practitioners, we developed two projects to encourage and facilitate such interaction, specifically: a) challenging hackathon competitions (project WPDP-C) developed collaboratively with our sibling Center of Excellence, the Center for Accelerating Operational Efficiency (CAOE) and b) continual development of meaningful internship, co-op and research experiences at the SENTRY academic labs and testbeds, HSE and DHS operational areas, and relevant industry and state and local organizations (project WPDP-D). Project WPDP-E will provide continuing education opportunities for first responders and HS professionals. Projects WPDP-A and WPDP-B will build pipelines with community colleges and minority serving institutions to encourage a diverse population of students and educators to consider employment and study of HS-related science and engineering disciplines.

In all the WPDP projects, an emphasis will be placed on broadening the participation of underrepresented communities. For example, SENTRY partner university, UPRM (an MSI) through the efforts of Dr. Samuel Hernandez, is engaged in the development and direction of several WPDP projects to ensure that a focus on building HS capacity within the MSI community is consistently front and center. Dr. Hernandez and the other WPDP project leads are building on existing MSI relationships to ensure diverse participation in all SENTRY WPDP projects. We have developed collaborations with the engineering societies serving women (SWE), Native Americans (AISES), African Americans (NSBE) and Hispanics (SHPE). They will disseminate information on SENTRY WPDP and research opportunities to seek applications and engagement and we are also exploring other ways that they could interact with our projects.

To evaluate the programmatic progress of the WPDP projects, we have adapted the DHS OUP stage-gate evaluation methodology to be more appropriate for education and workforce development. **Figure 3-1** illustrates the SENTRY WPDP Stage-Gate process. Due to the delay in funding for Year 1, this schedule shifted slightly for most projects from what we originally proposed. As shown, the projects begin Stage 1 of the process, Development and Planning. While this was expected to occur in Year 1, the delay in funding resulted in most of the project activity moving into Year 2. The next stage, the Pilot and Concept Refinements stage will occur in Year 2 for most projects. In that stage, each project will have conducted its initial major milestones (workshop, roundtable event, training session, module development) by the end of Year 2. During Year 2 or Year 3 depending on the project, the projects will enter Stage 3, Validate and Review Outcomes. This will allow for collecting performance metrics and analysis of the successes and needed improvement in each project. At the end of Year 3, all projects will enter into the final Stage 4, Replicate and Disseminate, which is when the improved and

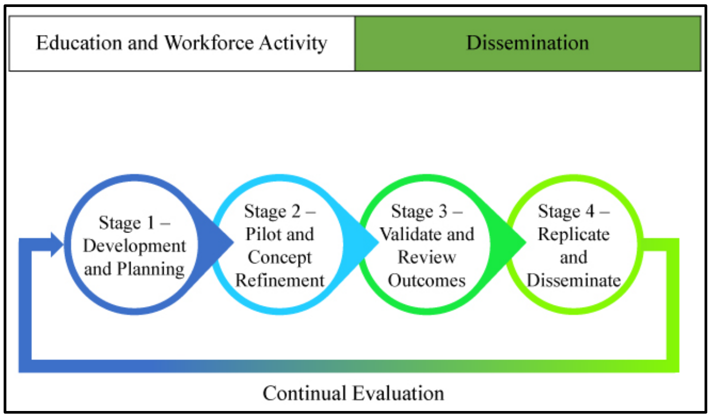
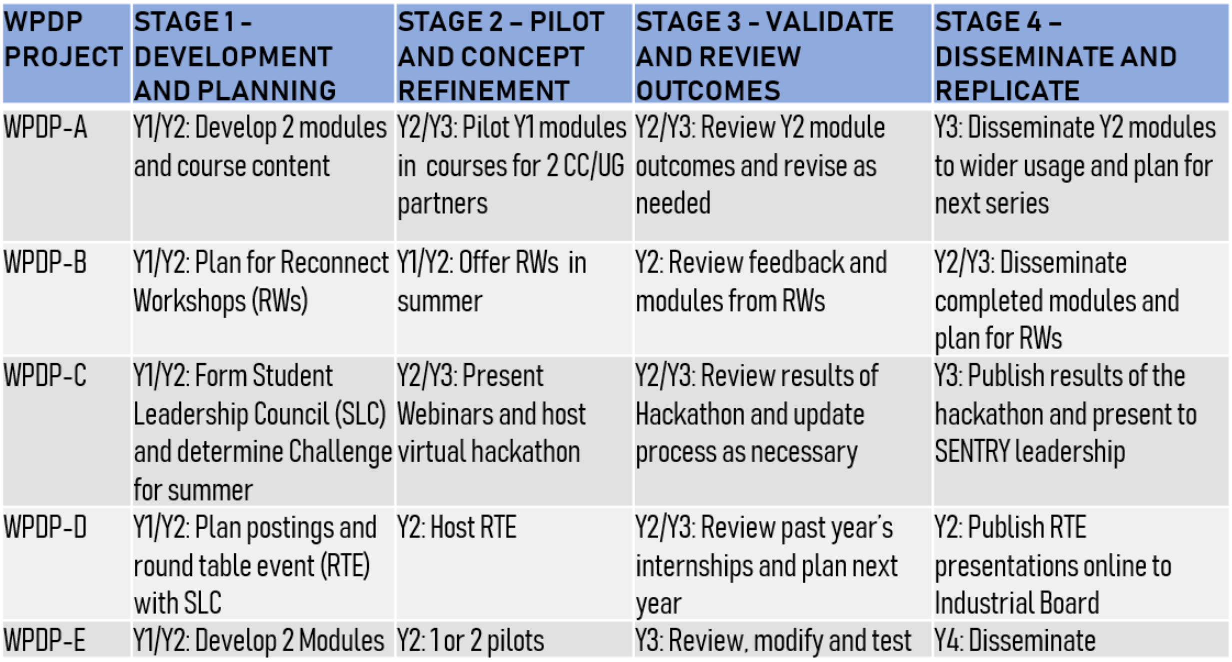

Education and Workforce Activity
Dissemination
Stage 1 – Development and Planning
Stage 2 – Pilot and Concept Refinement
Stage 3 – Validate and Review Outcomes
Stage 4 – Replicate and Disseminate
Continual Evaluation

***Figure 3-1**. SENTRY Workforce and Professional Development Program Stage-Gate Evaluation Process* refined version of the project will be commenced and, in the case of the instructional modules, disseminated for use in the classroom and enter the Pilot and Concept Refinement stage for that process. The WPDP projects will continually be evaluated post-dissemination as new directions for the projects will be considered. **Table 3-1** below provides a breakdown of the key workplan milestones expected for each WPDP project over the first two years (which will shift slightly due to late funding) and defined within the Stage-Gate methodology.

***Table 3-1**. Five WPDP projects and milestones.*



WPDP PROJECT	STAGE 1 - DEVELOPMENT AND PLANNING	STAGE 2 – PILOT AND CONCEPT REFINEMENT	STAGE 3 - VALIDATE AND REVIEW OUTCOMES	STAGE 4 – DISSEMINATE AND REPLICATE
WPDP-A	Y1/Y2: Develop 2 modules and course content	Y2/Y3: Pilot Y1 modules in courses for 2 CC/UG partners	Y2/Y3: Review Y2 module outcomes and revise as needed	Y3: Disseminate Y2 modules to wider usage and plan for next series
WPDP-B	Y1/Y2: Plan for Reconnect Workshops (RWs)	Y1/Y2: Offer RWs in summer	Y2: Review feedback and modules from RWs	Y2/Y3: Disseminate completed modules and plan for RWs
WPDP-C	Y1/Y2: Form Student Leadership Council (SLC) and determine Challenge for summer	Y2/Y3: Present Webinars and host virtual hackathon	Y2/Y3: Review results of Hackathon and update process as necessary	Y3: Publish results of the hackathon and present to SENTRY leadership
WPDP-D	Y1/Y2: Plan postings and round table event (RTE) with SLC	Y2: Host RTE	Y2/Y3: Review past year's internships and plan next year	Y2: Publish RTE presentations online to Industrial Board
WPDP-E	Y1/Y2: Develop 2 Modules	Y2: 1 or 2 pilots	Y3: Review, modify and test	Y4: Disseminate

The remainder of this section describes the development and planning that occurred in Year 1 (November 1, 2021 through June 30, 2022) for the five projects that constitute the SENTRY WPDP. These are: **WPDP-A** Community College and Undergraduate SENTRY Instructional Modules, **WPDP-B** Reconnect Workshop Series, **WPDP-C** SENTRY Student Leadership Council Hackathon, **WPDP-D** Internship/Co-op/Summer Research Experiences Pipeline, and **WPDP-E** First Responder Workforce Development Training Series. Each WPDP project report can be found in Appendix A.

3.2 WPDP-A: COMMUNITY COLLEGE AND UNDERGRADUATE SENTRY INSTRUCTIONAL MODULES

Principal Investigator: Margaret Cozzens, Distinguished Research Professor, Rutgers University

Theme area and Topic: Cross-Cutting

Goals, objectives and Year 1 Progress: The project goal is to develop instructional modules that bring security topics and techniques into Community College (CC) and undergraduate (UG) classrooms in a way that emphasizes the methods and tools of mathematics and computing and illustrates their role in planning for a secure environment. Although interdisciplinary themes are challenging to address in CC/UG curricula, the use of modules allows them to be flexibly included in various courses. Through the modules, CC/UG students learn foundational concepts in mathematical and computational sciences set in the context of issues relating to the security of STCPs. An online professional development mini-course accompanies each module to engage CC/UG faculty. The intent is to adapt and disseminate these modules for use by the SENTRY partners, other DHS COEs, and MSI CC/UG collaborators. Dr. Cozzens, lead for this project, has managed many module development projects, in areas such as bio-math, sustainability, computational thinking, and HS. She also developed online courses for the professional development of teachers on the topic of computational thinking. Since each of the modules developed for this project will relate to research topics in SENTRY, researchers will be recruited to help select the specific topics and review sections of the modules. The expectation is that two modules, along with the related online professional development course, will be created in Year 2. These Year 2 outputs will be piloted in Year 3 at which time the development of two more modules and related courses will be developed with the expectation to be piloted in Year 4. Additional modules will be created in the remaining years, with the number to be determined in Year 3. As of June 30, 2022, faculty participants who attend the RECONNECT workshop in Princeton, NJ were tasked with developing modules based upon the workshop focus of Optimization and how it might apply to the SENTRY mission. Module proposals are due in January 2023.

Capability or knowledge gap this project addresses and Year 1 update: CCs/UGs often do not have the resources to develop cutting edge courses that will help prepare their students for entry into the workforce. The modules will be made available to CCs/UGs free of charge, and the professional development will be offered by the course management system used, likely Canvas. CCs/UGs will be free to use these materials with any of their constituents, thus enabling wider access of topics to those interested in joining the DHS workforce while pursuing further education.

Alignment with and integration into the Center's research program: SENTRY researchers will be engaged in the decision about which research themes should be developed into instructional modules. They will also continue to be instrumental in creating the module instructional materials by advising the module writers and reviewing their output. Possible topics for modules include: 1) *An Introduction to Machine Learning (ML) and its use in Sensor Development, 2) Architectural Design of Layered Security Systems, 3) Operational Layered Surveillance of Large Crowds, 4) Game theory Applied to the Management of Surveillance Systems, and 5) Crowd-Optimized Design and Management of Environments.*

3.3 WPDP-B: RECONNECT WORKSHOP SERIES

Principal Investigator: Margaret Cozzens, Distinguished Research Professor Rutgers University

Theme area and Topic: Cross-Cutting

Goals, objectives and Year 1 progress: Reconnect Workshops (RWs) are a vehicle to foster the broad participation of underrepresented groups at CCs and MSI institutions in the SENTRY effort to protect STCPs. In Year 1, Optimization was the chosen topic for the workshop and the week-long event explored a variety of real-world applications that make use of optimization methods. SENTRY Researchers Carl Crawford of CSUPTWO LLC, and Jun Zhuang of the University of Buffalo provided overviews of SENTRY's research mission and offered examples of how they will use optimization methods in the center's research. These included allocating resources for disaster management, deploying "virtual sentries" to protect civilian spaces—so-called "soft targets"—around the country, and several others. The workshop will also lead to the development of the WPDP-A CC/UG instructional modules as the workshop participants will be submitting module drafts in January of 2023.

Capability or knowledge gap this project addresses and Year 1 update: CC/UG institutions often do not have the resources to develop cutting-edge courses or to provide significant professional development that will enable their faculty to learn and promote areas of study that are relevant to DHS and the HSE. Through participation in a focused workshop, the participating faculty can bring the concepts discussed and curricula developed to a broader base of students who could be interested in further exploration of the topics and their relationship to DHS and the HSE. Participants were faculty at five community colleges and five MSIs.

Alignment with and integration into the Center's research program: SENTRY researchers will assist in the determination of which research themes will be the subject of a week-long RW and will be engaged with the participants through presentations.

3.4 WPDP-C: SENTRY STUDENT LEADERSHIP COUNCIL HACKATHON

Principal Investigator: Michael Silevitch, Robert D. Black Professor, College of Engineering, NU

Theme area and Topic: Cross-Cutting

Goals, objectives and Year 1 progress: Each year, a Hackathon Committee (HC) will solicit possible themes from the four SENTRY Research Thrusts and select a topic such that will be part of a yearly hackathon challenge. Little planning was done in Year 1 due to the late start, but in Year 2, we initiated discussions with our sibling COE, the Center for Accelerating Organizational Efficiency (CAOE) and decide that this activity will be organized as a collaboration between the SENTRY and CAOE COEs. Planning for each event will begin with the solicitation of possible topics in the fall leading to the selection of three problem statements which will be presented at the weekend long event in February of 2023. The selection process would involve participation by industry, government, and academic partners as well as DHS component leadership. These subject matter experts and potential mentors will suggest informational webinar topics and speakers leading up to the event and ultimately, oversee the judging process for the hackathon submissions. The first Hackathon will take place in late February 2023.

Capability or knowledge gap this project addresses and Year 1 update: This activity will address the ability to narrow the knowledge gap that prevents creative problem-solving and an up-to-date needs assessment of the SENTRY research areas. The SENTRY PAB and IAB will also be participants in the planning and execution of the hackathons. In addition, DHS Components including, but not limited to, TSA, CBP, USCG, CISA, etc., would be involved as subject matter experts providing mentoring, resource material, webinar presentations and judges for the hackathon submissions.

Alignment with and integration into the Center's research program: The four SENTRY research thrusts and its overarching mission to protect STCPs are the sources of the Hackathon challenges.

3.5 WPDP-D: INTERNSHIP/CO-OP/SUMMER RESEARCH EXPERIENCES PIPELINE

Principal Investigator: Kristin Hicks, Director of Operations, NU

Theme area and Topic: Cross-Cutting

Goals, objectives and Year 1 progress: This project will facilitate and provide opportunities for graduate and undergraduate students to find interesting and challenging positions related to each of the SENTRY Research Thrusts in the COE labs and testbeds, HSE and DHS operational areas, as well as in relevant industry, state and local organizations. Multiple industrial and government collaborators have indicated their willingness to work with SENTRY students. This activity will maintain an updated "virtual bulletin board" of opportunities and a placement process for SENTRY student engagement in meaningful internship, co-op and research experiences. In Year 1, we began the development of the SENTRY website which will host this key listing. We expect to launch the new website in winter of 2023. In addition, SENTRY will hold an annual round table event where students, industry and government partners will network to publicize and plan for future opportunities and discuss successes and results of past opportunities. Planning for this activity will begin in the Fall of 2022 with the event to be held in either Spring or Fall 2023.

Capability or knowledge gap this project addresses and Year 1 update: This activity will address the critical capability gap of the difficulty faced by DHS leadership to maintain and engage a highly-skilled diverse workforce. It provides an exposure to talented and diverse graduate, UG and CC students familiar with the SENTRY academic disciplines and research areas. In Year 1, we began development of the website and in Year 2 will move to schedule events and postings related to this project.

Alignment with and integration into the Center's research program: Student engagement in internships, co-ops and summer research experiences embedded in relevant DHS components and other government or industry organizations will enhance their understanding of the relationship between the center and end-users while revealing possible extensions of SENTRY research themes. Also, students who embark on both DHS career opportunities and SENTRY research can act as ambassadors to introduce knowledge from one venue to the other.

3.6 WPDP-E: FIRST RESPONDER WORKFORCE DEVELOPMENT TRAINING SERIES

Principal Investigator: Jimmie Oxley, Professor of Chemistry, University of Rhode Island

Theme area and Topic: Cross-Cutting

Goals, objectives and Year 1 progress: Dr. Jimmie Oxley, lead for this project, has offered chemical and explosives hazard training to first responders for more than 15 years. Specifically, she worked with the TSA explosive specialists, training 50 a year for the past five years, and in the same period, she has offered training to another 1500 people in the HSE. For this project, building upon her significant body of training offerings, Dr. Oxley will work with other SENTRY researchers, first responders and DHS communities to identify the training areas with the greatest need to protect STCPs. The curriculum would include training on bomb prevention, active shooter response, current threats, new detection technologies, video and drone operation, decision making, legal considerations, first-aid, and various pseudo crises. In Year 1, Dr. Oxley attended meetings of the SENTRY Practitioner Advisory Board (PAB) in order to learn of their backgrounds, and to get insight on the capabilities and training needs for their respective domains. Based on the connections formed through that participation, she will be working with PAB members to identify areas that could be prime candidates for training to be offered in Year 2.

Capability or knowledge gap this project addresses and Year 1 update: This narrows the gap between DHS programs and the workforce in terms of sharing capabilities and up-to-date needs assessments. Discussions with the SENTRY PAB and others began in Year 1 and will lead to the determination of the types of training offerings to be made in Year 2.

Alignment with and integration into the Center's research program: The collaboration with the first responders will provide data and tactics to all of the SENTRY thrusts especially RA.

3.7 WPDP EVALUATION

The SENTRY WPDP projects will be reviewed in line with the center evaluation process described in Section 7 to ensure that they remain innovative, relevant to the SENTRY disciplines and integrated with the needs and requirements of DHS and the HSE.

Section 4: Technology Transition and Engagement

4.1 INTRODUCTION

The SENTRY transition strategy includes regular stage-gate-guided, metric-based project evaluations, stakeholder driven SWOTs (Strengths, Weaknesses, Opportunities, Threats), market and competitive landscape analyses, and project-transition partner matchmaking. In SENTRY's first year, the Transition Team focused on the goal of supporting SENTRY projects with tools and guidance to enable successful transition of technology to STCP security sectors. The efforts executed during this reporting period included: a) establishing relationships between the transition team and researchers; b) developing transition reporting tools and methods to ensure projects are evaluated equitably according to their developmental level; c) facilitation of DHS CAPO review; d) initiating the process of identifying and defining transition aspects of the SENTRY case studies to support the Virtual Sentry framework and build a SENTRY transition-focused stakeholder community; and e) support of initial end user/industry/government engagement.

4.2 BUILDING COMMUNICATION STRATEGIES AND RELATIONSHIPS

Year one began with establishing an administrative infrastructure for the transition team to support its work. An online collaboration space was created in Microsoft Teams to allow the team, which resides in different time zones, to work centrally and asynchronously as needed. The space includes a shared file system, task management system, real-time chat, and meeting space. The team established a recurring monthly meeting to define year one goals and tasks, review research projects, and collaborate on work.

To better serve individual SENTRY projects, the Transition Team decided to assign a specific team member to each project. This "Transition Liaison" will serve as the main point of contact for the project and serve in an on-call capacity to the PI as transition needs or questions on the project arise. This liaison reports out to the full transition team on ongoing project status and becomes a subject matter expert of sort for the project. See Table 4-1 for specific Transition Liaison project assignments.

The Transition Team performed an initial review of all SENTRY projects, reviewing workplan submissions, and project summaries. Assigned project transition liaisons held introductory calls with project PI's to introduce themselves and discuss the project's initial approach and milestones. Transition team members were tasked with identifying components or industries that may benefit from the project's work.

Table 4-1: Transition Liaison Assignments by Project

Project No.	Project Title	PI	Transition Liaison
RA - Real Time Threat Detection & Mitigation, Thrust Lead: David Castanon			
RA.1	Adaptive Layered Surveillance Systems: Design, Management and Decision Support for threat detection and mitigation	**Mario Sznaier**	**Desiree Linson**
RA.2	Low Complexity AI Based Fusion of Crowd-Sourced Heterogeneous Data Streams for Real-Time Threat Detection and Mitigation	**Eric Miller**	**Desiree Linson**
RA.3	Real time Video Surveillance for Threat Detection and Mitigation	**Rich Radke**	**Deanna Beirne**
RB - Advanced Sensing Technologies for Threat Awareness, Thrust Lead: Carey Rappaport			
RB.1	Multi-Sensor Threat Assessment Platforms	**Jimmie Oxley**	**Emel Bulat**

RB.2	Stationary and Aerial based RF/Radar Detection of Drones, Concealed Threats and Anomalous Communications	**Carey Rappaport**	**Emel Bulat**
RC - Threat Risk Assessment, Prediction & Deterrence, Thrust Lead: Jun Zhuang			
RC.1	Machine Intelligence for Effective Threat Deterrence and Risk Mitigation at Soft Targets and Crowded Places	**Auroop Ganguly**	**Isaac Maya**
RC.2	Protecting Soft Targets (ProSoT): A Game-theoretic Framework for Multi-target, Multi-layer Defense against Strategic Attackers	**Jun Zhuang**	**Deanna Beirne**
RD - Layered Security Architecture Design & Simulation, Thrust Lead: Michelle Laboy			
RD.1	Architectural Design Research: Integrating Security in the Public Realm	**Michelle Laboy**	**Deanna Beirne**
RD.2	Dynamic Digital Twin for Secure and Smart Civic Spaces	**Jie Gong**	**Isaac Maya**
RD.3	Real-Time Crowd and Attacker Forecasting for Risk Assessment and Threat Mitigation	**Mubbasir Kapadia**	**Isaac Maya**

4.3 SUPPORT OF CAPO REVIEW

A component of launching center projects is preparing materials for DHS Compliance Assurance Program Office (CAPO) review. Members of the Transition Team created a compliance matrix and evaluated each project to identify which SENTRY projects contain elements which would potentially fall under categories requiring CAPO review. The transition team members also developed a template for a project level Data Management Plan (DMP). Transition Liaisons held meetings with project PIs to review and clarify project details and discuss the development of project level DMPs. Out of the 10 projects, 6 SENTRY projects were identified as needing CAPO review and were validated as needing review by SENTRY's DHS Program Manager. Transition Liaisons held meetings with project PIs and Researchers to review CAPO submission requirements, explain the submission process, and identify deadlines for submission. The first project will be submitted for review in August, with other projects following on a rolling basis.

4.4 TRACKING AND REPORTING ON MILESTONES AND DELIVERABLES

To ensure project assessments align with the DHS Product Realization Guide (PRG)[i], the team developed templates for project transition reporting, annual reporting, and project workplans. By establishing uniform reporting templates, the Transition Team will have consistent data to clearly track progress and benchmark projects. Each template includes elements focused specifically on transition, and include TRL evaluation, milestone tracking, performance metrics, reporting on intellectual property, stakeholder engagements, and risk registers.

4.5 END USER PARTNERSHIPS

SENTRY has already begun establishing end user partnerships both at the center and project level. The center is supported by both a Policy-Practitioner Advisory Board (PAB), made up of a diverse cadre of STCP security stakeholders, and an Industrial Advisory Board (IAB), made up of businesses linked to the center by a membership model. Both the PAB and IAB are discussed further in Section 8 of this report. These boards give researchers a direct and ongoing link to STCP end users and industry. This guidance by experts in the STCP security space will ensure that work being done by SENTRY researchers will have a high likelihood of transition. As projects mature, members of the PAB will join with members of the IAB to participate in yearly SWOTs (Strengths, Weaknesses, Opportunities, and Threats) of SENTRY projects. In addition to the PAB, SENTRY has engaged with other end-users such as New York (NY) State Airports

(Buffalo and Albany), NY TSA, New Jersey Transit Authority, Customs and Border Protection (CPB) at the Port of Los Angeles/Long Beach, and various school security stakeholders this year.

SENTRY also pursues STCP security needs by regularly communicating with the DHS components, national laboratories, and industrial partners. There is an ongoing dialogue between our academic, government, and industrial partners at events such as the Advanced Development for Security Applications (ADSA) which focuses on the needs of the Transportation Security Administration (TSA) and Cybersecurity and Infrastructure Security Agency (CISA); Customs and Border Protection Advanced Developments Encompassing Processes and Technologies (CBP-ADEPT) Workshop which focuses on the needs of CBP; and COE directors' meetings. These events are discussed in more detail in Section 6**.**

4.6 CASE STUDIES

To facilitate the development of the Virtual Sentry framework, SENTRY has launched a series of case studies to assess the transition of its research into specific stakeholder venues. The ultimate intent of these case studies is to develop a pragmatic understanding of the needs associated with specific STCP venues and how those needs translate into an implementation of the Virtual Sentry system. SENTRY will develop case studies for STCP venues such as: a) schools (K-12); b) passenger-based surface transportation; c) sports arenas/events; d) shopping facilities; e) places of worship; and f) museums/cultural centers.

Each case study will commence with a moderated brainstorming session for the purpose of facilitating open discussion between SENTRY personnel and a panel of expert security stakeholders in the specified venue in order to gain preliminary understanding on how a Virtual Sentry system could best address the venue's safety and security concerns. Building on the information gathered from the brainstorming session, each case study will also host a focused ideation event with diverse representation from all relevant stakeholders within the venue, further generating concepts and ideas of how a Virtual Sentry framework may be structured in the space.

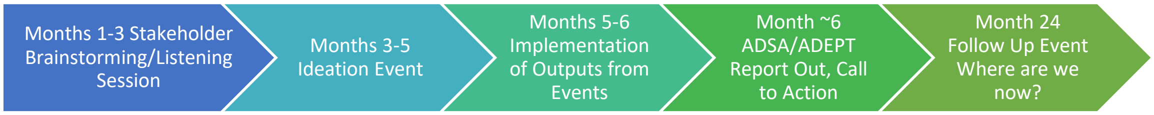
The outputs of the brainstorming session and focused ideation event will then be compiled and utilized to direct SENTRY's continued work regarding the case study. These two events will help inform SENTRY of the following for each venue:

- Security needs and priorities,
- Support center road mapping,
- Technology gaps in the current SENTRY portfolio,
- Pilots and partner venues,
- Ways to refine SENTRY research thrust areas and projects, and
- How to define Center RFPs

The outcomes and findings of these two events will be reported out to the SENTRY community at a subsequent workshop, providing further opportunity for government and industry stakeholder engagement and feedback. Lastly, the case studies will be revisited 24 months from initiation to reflect on progress in the space. Figure 4-1 outlines the proposed case study cycle.

In Year 1, SENTRY focused on the following case studies: School Security and Secure Surface Transportation. More details on these two initial case studies are given in Section 2.

Figure 4-1: Proposed SENTRY Case Study Cycle


Months 1-3 Stakeholder Brainstorming/Listening Session
Months 3-5 Ideation Event
Months 5-6 Implementation of Outputs from Events
Month ~6 ADSA/ADEPT Report Out, Call to Action
Month 24 Follow Up Event Where are we now?

4.7 ANNUAL PROJECT TRANSITION EVALUATIONS

The team has also been tasked with the evaluation of Year 2 Workplans and Year 1 Project Reports submitted for SENTRY semi-annual reporting. Due to the delayed start of funding, the first formal Project Transition Reviews are scheduled for early Fall of 2022.

4.8 CONCLUSION

In this first year, the Transition Team has established a strong foundation and process to support the transition successes of the SENTRY research portfolio and development of the Virtual Sentry framework. The team looks forward to continuing to engage with project PI's and external stakeholders to support SENTRY's critical mission. The team will regularly review project transition performance, pursue new opportunities for partnerships, and leverage our cohort of industrial members and HSE collaborators to move SENTRY technologies to market.

[i] Department of Homeland Security. (2013). https://www.dhs.gov/sites/default/files/publications/Product%20Realization%20Guide.pdf, accessed August 3, 2022.

Section 5: Industry Liaison and Partnerships Initiatives

5.1 INTRODUCTION

SENTRY's industry liaison and partnership initiatives expand on the highly successful strategies employed by the emeritus ALERT COE. These strategies proved to be key in developing and transitioning technologies that addressed the capability gaps outlined in the strategic objectives of DHS components. SENTRY has already begun building strong and mutually beneficial partnerships to address the challenges inherent in creating the Virtual Sentry (VS) framework to protect soft targets and crowded places by capitalizing on lessons learned from the ALERT COE.

5.2 INDUSTRY & GOVERNMENT PARTNERS

SENTRY's Industry Partners support the COE through donations, collaborating in joint proposals, and by providing internship, coop, and career opportunities for students. In addition, the Industry Partners provide access to research and development (R&D) leaders, real system-level applications, state-of-the-art hardware and software, and real applications data.

Industry Partners become members of the ALERT/SENTRY Industrial Advisory Board (IAB) and are recruited by two SENTRY Corporate and Government Liaisons, Emel Bulet and Desiree Linson. Through their recruiting efforts, four new Industry Partners have already been added to the IAB, while seven Industry Partners have been retained from ALERT, bringing the total ALERT/SENTRY IAB membership to eleven (see **Figure 5-1**). Two government laboratories also maintain collaboration with ALERT/SENTRY. The Corporate and Government Liaisons are responsible for engaging Industry and Government Partners in the COE's research and development efforts and seeking collaborative and transition opportunities that will advance the mission and provide solutions to the DHS Enterprise.

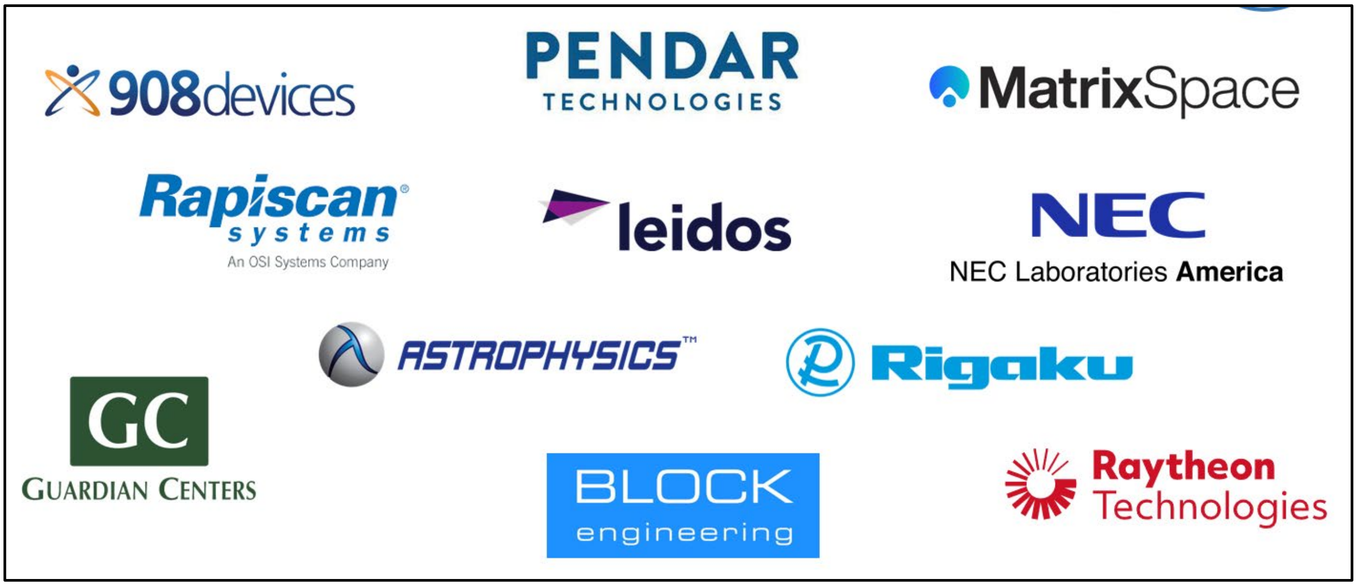


Figure 5-1: *ALERT/SENTRY Industrial Advisory Board (IAB) members for Year 1 of SENTRY.*

A. New Industry Partners

In Year 1, SENTRY's first year, the following four Industry Partners were brought in as new members of the ALERT/SENTRY IAB:

- **Block Engineering** has been a leader in the field of chemical detection and analysis for over 60 years. They supply laser-based spectrometers and mid-infrared quantum cascade lasers to researchers for early warning of toxic industrial chemicals, chemical warfare agents and other security and safety threats.
- **Leidos, Inc** is a global leader in the integration and application of information technology, engineering, and science to solve the customers' most demanding problems. Leidos makes the world safer, healthier, and more efficient through technology, engineering, and science. Leidos' key lines of business include civil, defense, health, and intelligence.
- **MatrixSpace** designs AI software that integrates optical, radar, lidar, thermal, and IR sensing used for autonomous systems such as smart drones and robots. Their distributed AI allows drones, cameras, and fixed security systems to compare information and situation awareness. In addition, it uses sensor, radar, and lidar capabilities to create ultra-detailed 4D maps of indoor and outdoor spaces.
- **NEC** has over 120 years of field-proven experience in creating IT and communication solutions. Their services and products include Advanced Recognition Systems, Unified Communications Platforms, and Emergency Notification Systems.

B. Retained ALERT Industry Partners

Seven Industry Partners from the ALERT COE were retained and have joined the ALERT/SENTRY IAB:

- **908 Devices** develops products ranging from rugged, handheld chemical detection tools to compact footprint analyzers and fast separation devices. These purpose-built and user-centric devices serve a range of industries including safety and security, oil and gas, life sciences, and other applied markets.
- **Astrophysics Inc.,** founded in 2002 by imaging scientist François Zayek, has since emerged as the industry innovator. With over thirty years in imaging technology, Mr. Zayek is experienced in both the medical and security industry. Mr. Zayek is joined by a team of field-leading scientists and software developers that transform theory into cutting-edge products. With a specific focus on security X-ray imaging and detection, Astrophysics delivers the best in technology.
- **Guardian Centers, LLC** is a disaster preparedness and tactical training center. Guardian Centers provides custom services including complete exercise design and planning, training and certification, and full-service logistics support at its state-of-the-art flagship training campus in Perry, Georgia, or at any client location throughout the world. Guardian Centers demonstrates exceptional performance and results delivering specialized training courses and practical exercises for special skills certification and professional services training. They are a total solutions company dedicated to testing, evaluating, and validating skills through training and exercise in dynamic and immersive urban terrain replicating the most realistic natural and manmade disasters.
- **Pendar Technologies** is a privately held product development company focused on bringing to market breakthrough portable analysis and monitoring systems that include proprietary data science driven analysis modules. With experts in innovative spectroscopy and data science, the company has a pipeline

of products in development. The company was formed by a merger of Pendar Medical and Eos Photonics in 2015.

- **Rapiscan Systems**, an OSI Systems Division, provides state-of-the-art security screening products, solutions, and services that meet the most demanding threat detection needs of customers worldwide, while improving operational efficiency. The technical staff at Rapiscan Laboratories, the R&D arm of Rapiscan Systems, is focused on leading edge physics, algorithm, and software-based research and development work in the detection of explosives, nuclear materials, and other contraband. Rapiscan recently merged with **American Science & Engineering (AS&E)**, specializing in detection technologies that can uncover dangerous and elusive threats. AS&E's X-ray inspection systems are used by governments and corporations around the world.
- **Raytheon Technologies** is focused upon accelerating ideas to solve some of the world's biggest challenges by bringing together the brightest, most innovative minds across aviation, space and defense. It forms an unrivaled company, with one team coming together across the globe to push the limits of known science and redefine how we connect and protect our world. The company is advancing aviation, building smarter defense systems and creating innovations to take us deeper into space.
- **Rigaku Analytical Devices** is a leading pioneer and innovator of handheld and portable spectroscopic analyzers for use in the protection of public health and safety, aid in the advancement of scientific and academic study, enable the recycle and reuse of metal alloys, and ensure quality of key metal alloy components in mission-critical industries. Their advanced and rugged products deliver unparalleled accuracy and extensive application support, empowering their customers to achieve rapid lab-like results any time, any place.

C. Government Collaborations

Government Partners lend their expertise and collaborate on research projects. ALERT/SENTRY maintains collaborations with two government laboratories:

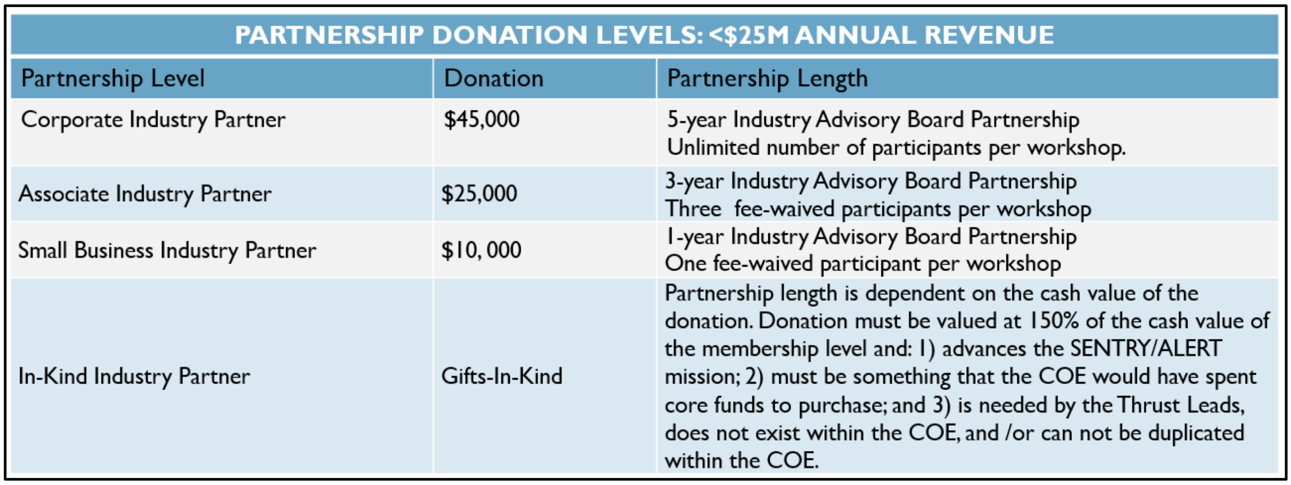
- **Lawrence Livermore National Laboratory** (LLNL) is a premier research and development institution for science and technology applied to national security. They are responsible for ensuring that the nation's nuclear weapons remain safe, secure, and reliable. LLNL also applies its expertise to prevent the spread and use of weapons of mass destruction and strengthen homeland security.
- **Pacific Northwest National Laboratory** (PNNL) is one of the U.S. Department of Energy's (DOE's) ten national laboratories, managed by DOE's Office of Science. PNNL also performs research for other DOE offices as well as government agencies, universities, and industry to deliver breakthrough science and technology to meet today's key national needs.

5.3 IAB MEMBERSHIP STRUCTURE AND BENEFITS

A. Partnership Donation Levels

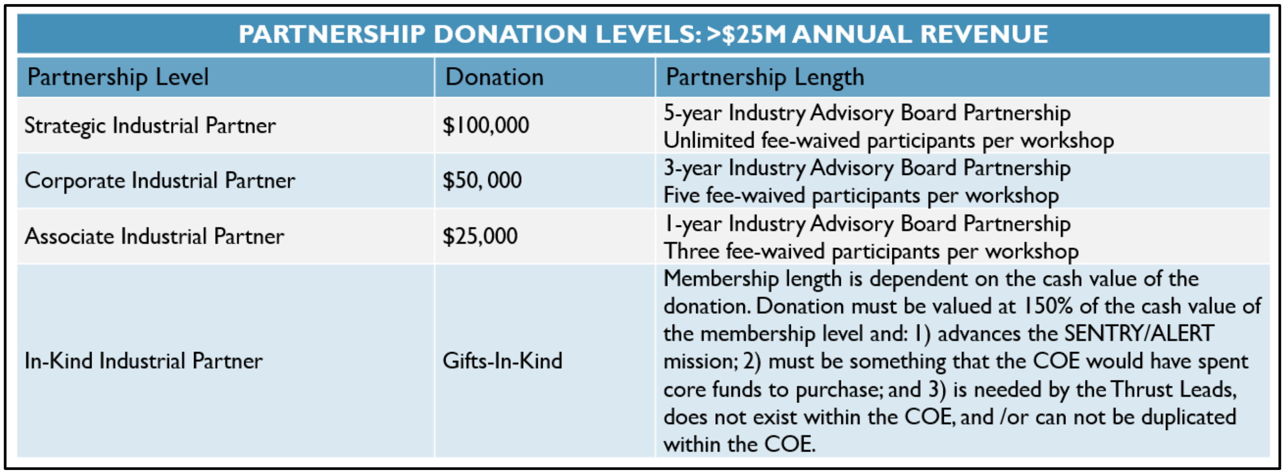
The ALERT/SENTRY Industrial Advisory (IAB) is comprised of industry partners whose expertise align with and can advance the research and development mission of SENTRY. Industry Partners are strategically recruited and required to donate funds to augment the core funding provided by DHS. The donated funds from the Partners provide SENTRY the flexibility to support additional research as more is discovered about protecting soft targets and crowded places. In addition, in lieu of funds, SENTRY accepts in-kind donations of hardware and software that otherwise would have been purchased using core DHS funding.

IAB membership levels are based on the annual revenue of the Industry Partner. Partners with less than $25 million in revenue donate $10K, $25K, or $45K. Those that exceed $25 million in revenue annually donate at the $25K, $50K, or $100K levels. Each donation level has a corresponding number of membership years associated with it (See **Tables 5-1 and 5-2**). Past experience with the ALERT COE revealed that Industry Partners who donate are incentivized to engage more closely with the research efforts of the COE.



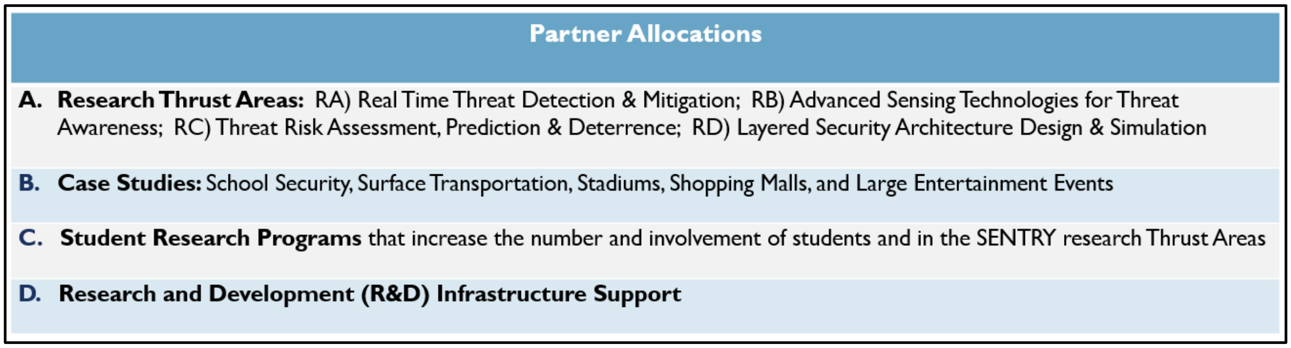
PARTNERSHIP DONATION LEVELS: <$25M ANNUAL REVENUE		
Partnership Level	Donation	Partnership Length
Corporate Industry Partner	$45,000	5-year Industry Advisory Board Partnership Unlimited number of participants per workshop.
Associate Industry Partner	$25,000	3-year Industry Advisory Board Partnership Three fee-waived participants per workshop
Small Business Industry Partner	$10, 000	1-year Industry Advisory Board Partnership One fee-waived participant per workshop
In-Kind Industry Partner	Gifts-In-Kind	Partnership length is dependent on the cash value of the donation. Donation must be valued at 150% of the cash value of the membership level and: 1) advances the SENTRY/ALERT mission; 2) must be something that the COE would have spent core funds to purchase; and 3) is needed by the Thrust Leads, does not exist within the COE, and /or can not be duplicated within the COE.

Table 5-1: *ALERT/SENTRY IAB partnership donation levels for partners with less than $25 million in revenue.*



PARTNERSHIP DONATION LEVELS: >$25M ANNUAL REVENUE		
Partnership Level	Donation	Partnership Length
Strategic Industrial Partner	$100,000	5-year Industry Advisory Board Partnership Unlimited fee-waived participants per workshop
Corporate Industrial Partner	$50, 000	3-year Industry Advisory Board Partnership Five fee-waived participants per workshop
Associate Industrial Partner	$25,000	1-year Industry Advisory Board Partnership Three fee-waived participants per workshop
In-Kind Industrial Partner	Gifts-In-Kind	Membership length is dependent on the cash value of the donation. Donation must be valued at 150% of the cash value of the membership level and: 1) advances the SENTRY/ALERT mission; 2) must be something that the COE would have spent core funds to purchase; and 3) is needed by the Thrust Leads, does not exist within the COE, and /or can not be duplicated within the COE.

Table 5-2: *ALERT/SENTRY IAB partnership donation levels for partners with more than $25 million in revenue.*



Partner Allocations
A. Research Thrust Areas: RA) Real Time Threat Detection & Mitigation; RB) Advanced Sensing Technologies for Threat Awareness; RC) Threat Risk Assessment, Prediction & Deterrence; RD) Layered Security Architecture Design & Simulation
B. Case Studies: School Security, Surface Transportation, Stadiums, Shopping Malls, and Large Entertainment Events
C. Student Research Programs that increase the number and involvement of students and in the SENTRY research Thrust Areas
D. Research and Development (R&D) Infrastructure Support

Table 5-3: *ALERT/SENTRY IAB Partner Allocation options.*

B. Allocation of Donated Funds

Industrial Partners can choose amongst four different options on how to allocate their donations: a) Research Thrust Areas; b) Case Studies; c) Student Research Programs; and/or d) Research and Development (R&D) Infrastructure Support (see **Table 5-3**). All donations further support SENTRY in its research in protecting STCPs.

C. Membership Benefits

Industrial Partners have access to several benefits as part of their membership with ALERT/SENTRY, including:

- Faculty Researchers & Transition Opportunities
  - Facilitation of joint proposals
  - Development of sponsored (proprietary) research contracts
  - Subcontracts for Task Orders under the Basic Ordering Agreement (BOA)
- SENTRY Students
  - Undergraduate and graduate co-op assignments
  - Internships
  - Fellowships
- Testbed Facilities (see Section 2 for more details)
  - Northeastern University (NU) Expeditionary Cyber and Unnamed Aerial System (ECUAS) Lab Offense and Defense Facility
  - NU Colosseum 5G/6G Agile Communications Facility
  - Rutgers Living Lab Public Venues with Digital Twin
  - Guardian Centers Realistic Rail, Infrastructure Training Facility
- Datasets
  - CT Segmentation Dataset
  - Reconstruction Initiative Dataset
  - Automated Threat Recognition (ATR) Dataset
  - Airport Re-Identification Dataset
- Networking
  - DHS Components
  - Other Federal Agencies and Labs
  - Other Industrial Partners
- Fee-Waived Workshops
  - Advanced Development of Security Applications (ADSA)
  - Advanced Developments Encompassing Processes and Technology (ADEPT)

- Members-only Events
    - **Annual Student Pipeline to Industry Roundtable Event (ASPIRE) -** This event brings students, Industry Partners, and Government Partners together with a threefold intent. First, ASPIRE is designed to introduce Industry Partners to highly qualified students seeking internships, coops or permanent positions. Second, government sponsors from DHS components and government labs are invited to the event to give career advice to the student participants. Third, information obtained from student participants is added to the SENTRY Candidate Central Portal, which is a password-protected portal on the SENTRY/ALERT website that provides Industry Partners access to biographies and resumes of exceptional SENTRY students and recent graduates who are interested in homeland security related jobs or internships.
    - **Industrial/Government Advisory Board (IAB) Meeting** – The IAB meeting focuses on awareness of the SENTRY mission and providing a networking opportunity for faculty researchers, Industry Partners, and Government Partners to develop relationships that will facilitate technology transfer and other collaborative efforts. The meeting agenda may include guest lecturers, in-depth faculty presentations, Industry Partner presentations, tours of testbeds, and a student/faculty research poster session.
    - **Annual Project Review** – This event provides Industry Partners with up-to-date information on the progress of all SENTRY research projects and gives them an opportunity to provide feedback, identify transition opportunities, and collaborative efforts.
    - **Technology Demonstrations & Other Special Events** – To expand SENTRY's footprint, a series of bi-annual special events will be conducted, such as the ALERT Technology Demonstration event that was held in conjunction with CBP at the Los Angeles/Long Beach Seaport on November 21, 2019. These events will be held at various locations, such as southern California and New Jersey, and focus on specific topics such as supporting CBP in designing and building a state-of-the art Command Center that includes next-generation resource allocation modeling, video analytics, human detection sensors, radiation portal monitoring and encrypted 5G connectivity. In Year 2, SENTRY-partner, ALERT hosted field trial for a human detection sensor on the Southern California Seacoast on July 8, 2022 and a Command Center workshop on July 11-13, 2022.

5.4 CONCLUSION

The SENTRY industry liaison and partnership initiatives provide the critical infrastructure needed to build a bridge from research to reality. Lessons learned from the emeritus ALERT COE have shown that strong relationships between Industry Partners, Government Partners, researchers, and students yield concrete solutions to the challenges faced by DHS in protecting the homeland. These partnerships are cultivated by: a) funds provided by Industry Partners, b) engaging all partners in the on-going research through attendance at meetings, workshops, and conferences (virtually and in-person) that provide one-on-one interaction and, c) providing career opportunities for the next generation of homeland security experts.

Section 6: SENTRY Strategic Workshops & Events

6.1 INTRODUCTION

Part of SENTRY's mandate from the Department of Homeland Security (DHS) is to develop a strategy to identify gaps in the knowledge for effective protection of Soft Targets and Crowded Places (STCPs). To help address this need, SENTRY will modify and continue its flagship ALERT Advanced Developments for Security Applications (ADSA) conferences and develop other events to foster this objective. This section of the Annual Report will discuss both the ADSA workshops as well as the events that will enable effective implementation of the SENTRY case studies defined in Section 2 of this report.

6.2 ADSA WORKSHOPS

The ADSA workshops have been, and will continue to be, valuable in creating collaborative opportunities by engaging participants from industry, national labs, vendors, government, and academia in an integrated setting where the Center acts as a neutral broker. This is vital in the further development of a dynamic network that can foster the innovative basic research, education, and technology needed to help DHS in its mission to help safeguard our nation.

To that end, an initial SENTRY-oriented ADSA workshop was held on May 3-4, 2022, supplementing the 24 workshops in this series held previously under ALERT. The theme of this workshop was Protecting Surface Transportation and Other Soft Targets. The topics covered at this event are listed in the table below. As shown in Table 6-1, the invited presenters represent the multiple stakeholders needed to achieve the SENTRY mission.

***Table 6-1**: ADSA25 Agenda*

DHS, TSA, CISA and Other Overarching Perspectives	
Keynote Address *[In person]*	**Austin Gould** *Acting Deputy Executive Assistant Administrator for Operations Support, Transportation Security Administration*
Protecting Surface Transportation *[In person]*	**Sonya Proctor** *Assistant Administrator for Surface Operations Transportation Security Administration*
TSA Topics relating to protecting soft targets *[In person]*	**Keith Goll** *Acting Assistant Administrator for Requirements and Capability Transportation Security Administration*
DHS's Cybersecurity and Infrastructure Security Agency (CISA): Introduction and Role in Protecting Soft Targets *[Virtual]*	**David Mussington** *Assistant Director for Infrastructure Security DHS Cybersecurity and Infrastructure Security Agency (CISA)*
DHS S&T Activities on Soft-Target Protection *[In person]*	**Ali Fadel** *Physical Security Program Manager Soft Targets Security Science & Technology Directorate U.S. Dept. of Homeland Security* **Patrick LaFontant** *Support Contractor Science and Technology Directorate Department of Homeland Security*
FBI's Perspective on Protecting Soft Targets *[In person]*	**Kirk Yeager** *Chief Explosives Scientist Federal Bureau of Investigation*
Terrorism and Sophisticated Crime *[Virtual]*	**Brian Michael Jenkins** *Director, National Transportation Security Center Mineta Institute & Rand Corporation*
NCITE's (DHS Center of Excellence) Perspective on Protecting Soft Targets *[In person]*	**Gina Ligon** *Director of NCITE COE University of Nebraska Omaha*

Case Studies: Schools and Sports Venues	
What Worried This High School Principal? *[In person]*	**Jacob Ludes** *CEO and President New England Association of Schools and Colleges (Retired)*
Securing Jewish Institutions *[In person]*	**Ari Friedman** *Director of Security & Community Properties Milwaukee Jewish Federation*
Architectural Design for Protecting Soft Targets *[In Person]*	**David Fannon** *Associate Professor School of Architecture Northeastern University*
Balancing Stakeholder Needs for Protecting Schools *[Virtual]*	**Rabbi Mendel Shmotkin** *CEO Lubavitch of Wisconsin*
Security for NFL Venues *[In Person]*	**Cathy Lanier** *Chief Security Officer National Football League*
Application of Serious War Gaming to Protecting Soft Targets for Developing Concepts of Operation and Requirements *[Virtual]*	**Diederik Stolk** *Founding Partner Goldsworthy, Stolk & Associates*
Case Studies - Part II	
Humans Are the Weakest Link in Security - But Also Could Be the Greatest Asset! *[In person]*	**Jennifer Hesterman** *Colonel, USAF (retired) Vice President Watermark Risk Management International*
Being a Night Watchman When Protecting Soft Targets - Dealing with Rare Events *[Virtual]*	**Jeremy Wolfe** *Professor of Ophthalmology & Radiology Harvard Medical School*
Optimizing Multi-Layered Security Screening [Virtual]	**David Anderson** *Transport & Border Security Joint Research Centre (JRC) European Commission*
Validating Adaptive Behavior Models of Adversaries for Risk Assessment [Virtual and In Person]	**Brandon Behlendorf** *Deputy Director, Center for Advanced Red Teaming Assistant Professor Homeland Security & Cybersecurity University at Albany State University of New York* **Gary Ackerman** *University at Albany State University of New York*
Active Shooter Drills at Logan Airport [In person]	**Wendy Riggs-Smith** *Senior Project Manager Massachusetts Port Authority*
Security at the Mall of America [In Person]	**Will Bernhjelm** *Vice President Security, Mall of America*
Balancing Stakeholder Needs for Protecting Synagogues *[Virtual]*	**Rabbi Wesley Kalmar** *Anshe Sfard Kehillat Torah Synagogue Milwaukee, Wisconsin*
Industrial Experiences	
Qylur's Experiences with Venue Protection *[In person]*	**Lisa Dolev** *Founder & CEO Qylur Security Systems*
Evolv's Experiences with Venue Protection *[In person]*	**Michael Ellenbogan** *Founder & Chief Innovation Officer Evolv Technology*
Leidos' Products for Protecting Soft Targets *[In person]*	**Andrew Foland** *Chief Technical Officer Leidos*
Radar-based Threat Detection for Soft Target Applications *[In person]*	**Ajay Subramanian** *Principal RF Design Engineer Liberty Defense* **Michael Lanzaro** *President and CTO Liberty Defense*
TSA - Soft Targets and Aviation Security	
TSA Perspective on Protecting Soft Targets *[In person]*	**Matt Gilkeson** *Innovation Task Force Division Director Transportation Security Administration*
Emergent Challenges in Aviation Security that Drive the Need for Enhanced Detection	**Don Kim** *Senior Aviation Security Systems Engineer Transportation Security Administration*

Equipment *[In person]*	
Technology Development	
From EMI to AI: a Brief History of Commercial CT Reconstruction Algorithms - Emphasis on Driving Forces *[Virtual]*	**Patrick La Riviere** *Professor* *Department of Radiology* *The University of Chicago*
Black Box AI and DHS Systems *[In person]*	**Matthew Merzbacher** *Volunteer Alameda County Community Food Bank*
Automation Reliability, Human-Machine System Performance and Operator Compliance: A study with Airport Security Screeners *[In person]*	**David Huegli** *Research Scientist University of Applied Sciences and Arts Northwestern Switzerland*
School Safety	
Modeling and Simulation for Improved School Safety [In person]	**Robert Hanson** *Deputy Associate Program Leader for Defense Infrastructure, Global Security E Program, Lawrence Livermore National Laboratory (LLNL)* **Amy Askin** *Global Security Systems Analyst, LLNL*

6.3 CASE STUDY EVENTS

In addition to the ADSA workshops, SENTRY will organize events supporting specific case studies in STCP areas such as school security. SENTRY has launched a series of case studies to assess the transition of its research into specific stakeholder venues. The ultimate intent of these case studies is to develop a pragmatic understanding of the needs associated with specific STCP venues and how those needs translate into an implementation of the VS system. In Year 1, SENTRY focused on the following case studies: School Security and Secure Surface Transportation. To date, the preparation for these case studies is as follows:

School Security

The School Security case study is being driven by the expertise inherent in the SENTRY Policy-Practitioner Advisory Board (PAB) – namely Jacob Ludes, Former President/CEO of the New England Association of Schools and Colleges, who has extensive experience with and knowledge of school security needs and best practices that qualify him to guide this effort. In Year 1, SENTRY took the following steps regarding the school safety case study:

A. SENTRY School Security Case Study Working Group

   An initial working group of 20 SENTRY personnel assembled February 2022 to address the school security case study, meeting bi-weekly to discuss the problem statement and define the next steps SENTRY should take in order to successfully implement the VS system in school venues.

B. SENTRY School Security Brainstorming Session

   On April 12, 2022, SENTRY hosted a 3-hour School Security Brainstorming Session, held virtually via Zoom, for the purpose of facilitating open discussion between SENTRY personnel and five school security stakeholders on how a Virtual Sentry (VS) could best address safety concerns for K-12 school venues. The invited school security panelists included:

   - Dr. George Edwards, Director of Accreditation, New England Association of Schools and Colleges

- Dr. Joseph Erardi, Superintendent (retired), Newtown, Connecticut, Public Schools
- Dr. Penelope (Penny) Eucker, Executive Director, STEM School, Highlands Ranch, CO
- Dr. Lawrence Filippelli, Superintendent, Lincoln Public Schools, Lincoln, RI; President/Proprietor, The Education Consortium
- Dr. Kevin McCaskill, Senior Administrator Secondary Schools, Boston, Massachusetts, Public Schools

The following points of discussion were distributed to participants in advance of the meeting to guide the conversation:

- School/campus areas or locations of concern
- Privacy issues which imposed limitations on security actions or installations
- Countermeasures/detection capabilities installed or desired
- Architectural impacts/solutions for new designs or retrofitted in schools
- Deterrence; is it a meaningful factor, and how is it accomplished?
- What are the best practices/drills to prepare for threats or such incidents?
- How can CCTV and classroom televisions be used for school security?

SENTRY personnel summarized the key takeaways from the session in an internal report that will be utilized to inform SENTRY's continued work regarding the school security case study. The session also established connections with key school stakeholders that SENTRY plans to develop into partnerships in assessing the utility of the VS system.

C. Future of School Security Working Meeting

Building on the information gathered from the School Security Brainstorming Session, SENTRY in Year 2 hosted the Future of School Security Meeting in collaboration with Pacific Northwest National Laboratories (PNNL). The meeting was an invitation-only moderated collaboration which allowed for an open exchange of ideas on the art of the possible with respect to the future of school security. 37 external participants were specifically selected based on their experience and expertise, with stakeholder representation from SENTRY researchers, first responders, school security personnel, teachers, school administrators, phycologists/social workers, technologists, DHS components, parents, and students. Year 1 funding of $45K was allocated to support this ideation event, which took place virtually in two 4-hour sessions on July 19 and 21, 2022.

PNNL will collate the feedback gathered at this Futures meeting into a final report and detail recommendations on technologies, requirements and priorities of a VS framework in the school security space. SENTRY will incorporate the findings from this report as we continue work on the school security case study.

In Year 2, specific venues will be identified to assess the utility of the VS system approach. Funding will be allocated from the $1M Year 2 SENTRY Plus-up funds to support this effort.

Secure Surface Transportation

The Secure Surface Transportation case study is being driven by the prior work that Prof. Jie Gong and the Rutgers CICCADA COE have done in collaboration with the New Jersey Transit Authority. Specific steps for the SENTRY research team to learn about the problem in Year 1 included the following:

A. Meeting with the New Jersey Transit Authority

   On May 9, 2022, a meeting took place between SENTRY personnel and the New Jersey Transit Authority to discuss the development of a collaboration to enhance the resilience of the facility to withstand both man-made as well as natural threats. The outcome was an agreement to work together toward understanding of their problems and the creation of a meaningful VS framework. Jie Gong and Fred Roberts from Rutgers and CICCADA, along with George Naccara and other members of the PAB, will lead the effort.

B. Meeting with TSA Stakeholders

   George Naccara initiated conversations with Sonya Proctor, Assistant Administrator for Surface Operations, Transportation Security Administration (TSA) and other TSA personnel to discuss the Secure Surface Transportation case study and the Rutgers/New Jersey Transit project and possible SENTRY/TSA collaboration. Both parties agreed that SENTRY should utilize existing TSA surface transportation testbeds as initial venues, with Hoboken/New Jersey Transit Terminal as one of those testbeds. SENTRY plans to initiate similar conversations with Cybersecurity and Infrastructure Security Agency (CISA) stakeholders to explore other possible collaborations.

C. Secure Surface Transportation Brainstorming Session

   SENTRY is planning a brainstorming session for fall 2022 to explore the Secure Surface Transportation case study. The format of this session will be similar to the School Safety Brainstorming Session that took place spring 2022. Proposed participants include representatives from the following:

   - Los Angeles County Metropolitan Transportation Authority
   - Massachusetts Bay Transit Authority
   - New Jersey Transit
   - New Orleans Regional Transit Authority
   - Washington Metro

   SENTRY plans to initially focus on the Hoboken/New Jersey Transit Terminal to examine the compounding of threats from man-made attacks and natural hazards. The effort will create a strategy to link with the other existing TSA Requirements and Capability Analysis (RCA) transportation testbeds that are part of a national surface security technology field testing partnership.

In Year 2, SENTRY will identify specific venues to assess the utility of the VS system approach. Funding will be allocated from the $1Million Year 2 SENTRY Plus-up funds to support this effort.

6.4 CONCLUSION

This section of the Annual Report dealt with the development of workshops and events to further engage a wide range of stakeholders in the mission of SENTRY. The ADSA and case study events are just the beginning.

As SENTRY matures, there will be Task Orders and other opportunities to implement specific manifestations of the Virtual Sentry, which is the system-level goal of the COE. These will be defined and discussed in future reports to DHS.

Section 7: Management and Evaluation

The technical challenges outlined in the SENTRY program are significant. Overcoming the underlying research barriers requires fundamentally new approaches. Effectively managing and evaluating the outcomes of this complex enterprise presents a challenge equal to the basic research challenges themselves. To support this effort, the SENTRY management team is comprised of faculty and staff from the core partners and augmented by our partnership with national labs, companies, and government agencies. We understand that each entity within the Center must maintain its own unique charter and work environment while also striving for coherence. In this section, we first discuss the SENTRY organizational structure, followed by the processes for evaluating the SENTRY research, transition projects, and outcomes. Both are needed to ensure continued relevance of the Center of Excellence (COE) to the DHS mission.

7.1 MANAGEMENT APPROACH

A. SENTRY Organizational Structure and Leadership Team

SENTRY will be led by an effective, experienced cross-campus team that will leverage a broader network of national advisors to ensure relevance of SENTRY activities. Nearly all members of this leadership team have participated in the ALERT DHS COE since 2008. The experience and infrastructure that have been developed through these existing Center components will be invaluable for managing SENTRY. In addition to the key leadership, experienced administrative and professional support staff are on hand to address the detailed needs of the COE. The SENTRY organizational structure has been designed to support the oversight, planning and coordinating activities of the multi-faceted COE**.** This is shown in **Figure 7-1**.

As the organization chart indicates, leadership and responsibilities stem from the **Director** and **Deputy Director** who will have overarching fiscal and technical oversight of the COE and interface directly with the DHS Program Manager. An **Executive Committee** will be responsible for coordinating, integrating and monitoring the progress and timeliness of the SENTRY research, transition and education efforts. Its members include eight program leads – one for each research area, one for education and workforce development, and three for transition – who report to the Director and Deputy Director. **Policy-Practitioner and Industry Advisory Boards** are made up of world-class experts in the specific challenges of STCPs and leading commercial firms who will guide SENTRY activities. A highly experienced **Administrative Staff** will manage all operational aspects of the COE with oversight from the Director (i.e. financial/resource management, communications and outreach, program/project evaluation, education/workforce development, and technology transfer/transition).

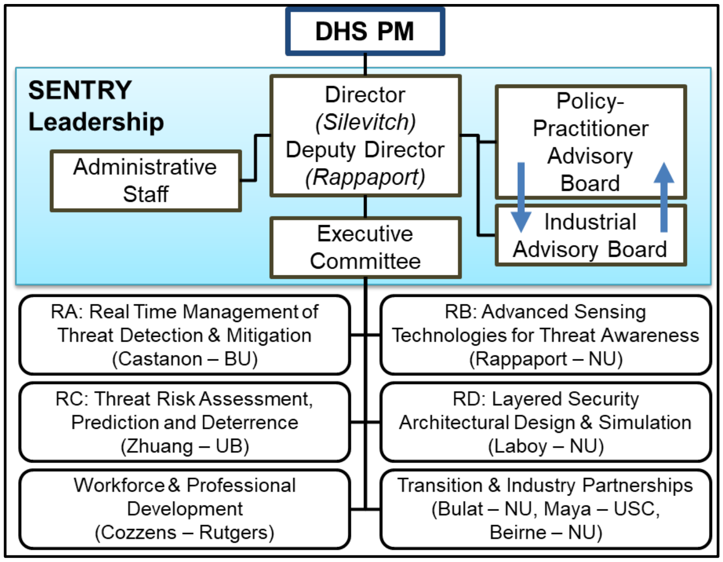

DHS PM
SENTRY Leadership
Director (Silevitch) Deputy Director (Rappaport)
Administrative Staff
Policy-Practitioner Advisory Board
Industrial Advisory Board
Executive Committee
RA: Real Time Management of Threat Detection & Mitigation (Castanon – BU)
RB: Advanced Sensing Technologies for Threat Awareness (Rappaport – NU)
RC: Threat Risk Assessment, Prediction and Deterrence (Zhuang – UB)
RD: Layered Security Architectural Design & Simulation (Laboy – NU)
Workforce & Professional Development (Cozzens – Rutgers)
Transition & Industry Partnerships (Bulat – NU, Maya – USC, Beirne – NU)

Figure 7-1. *The SENTRY Organizational Structure for both the leadership and management of the COE, shown in blue, as well as the interface with the SENTRY research, education and workforce development, and transition activities.*

B. Director and Deputy Director

Professor Michael Silevitch, SENTRY Director, oversees and is responsible for all COE activities in a full-time capacity, working closely with the DHS Program Manager (PM). Professor Silevitch has been Director of the ALERT DHS COE from 2008-2021 and was PI/Director of the Bernard M. Gordon Center for Subsurface Sensing and Imaging Systems National Science Foundation Engineering Research Center (Gordon-CenSSIS) from 2000 to 2010. He brings nearly 40 years of leadership and management experience in large, multi-institution, multi-task, high-stakes initiatives similar to the SENTRY DHS COE. He was also the PI of two large research and transition-oriented DHS projects relating to the detection of nuclear and explosive threats.

Professor Carey Rappaport, SENTRY Deputy Director, will support Dr. Silevitch in general oversight of the COE, with emphasis on the technical oversight of the research activities. Dr. Rappaport serves as Associate Director of Gordon-CenSSIS and, as of January 2022, Director of ALERT (before that, he served as the Deputy Director for ALERT). He has 20+ years of experience with the managerial aspects of running multi-institution academic centers. Dr. Rappaport will also oversee Research Thrust RB.

Drs. Silevitch and Rappaport have worked closely together for over 30 years on ALERT, Gordon-CenSSIS and other activities, and presently Dr. Rappaport serves as Deputy Director of ALERT. Their offices are co-located in the current ALERT headquarters and they are in daily contact which will continue to ensure all COE management and administration is handled smoothly, including timely provision of all COE publications, progress reports, and other documentation to DHS. They will allocate and prioritize resources in close coordination with the DHS PM and in concert with the Evaluation processes needed by the Center.. Assisted by the Executive Committee and project leads, they will facilitate interactions and collaboration between investigators and students in the COE and across COEs.

C. Executive Committee

The Executive Committee shown in **Figure 7-1** will be responsible for coordinating, integrating and monitoring the progress and timeliness of the SENTRY research, transition and workforce and professional development efforts. Their responsibilities include:

- Managing and monitoring the technical quality of the projects and maintaining active communication with and between the participants (researchers, students, collaborators) on the different research projects and other COE activities.
- Actively facilitating the dissemination of outcomes (e.g. linking with government, industry and practitioner partners to expedite the translation of knowledge, both through the Industrial and Policy-Practitioner Advisory Boards and beyond)
- Ensuring integration of projects.
- Program scheduling, documentation, reporting and assessment. The Executive Committee will be responsible for developing the annual report in coordination with Director, Deputy Director and staff.
- Providing input as to appropriate funding or pruning of each project or proposed project.

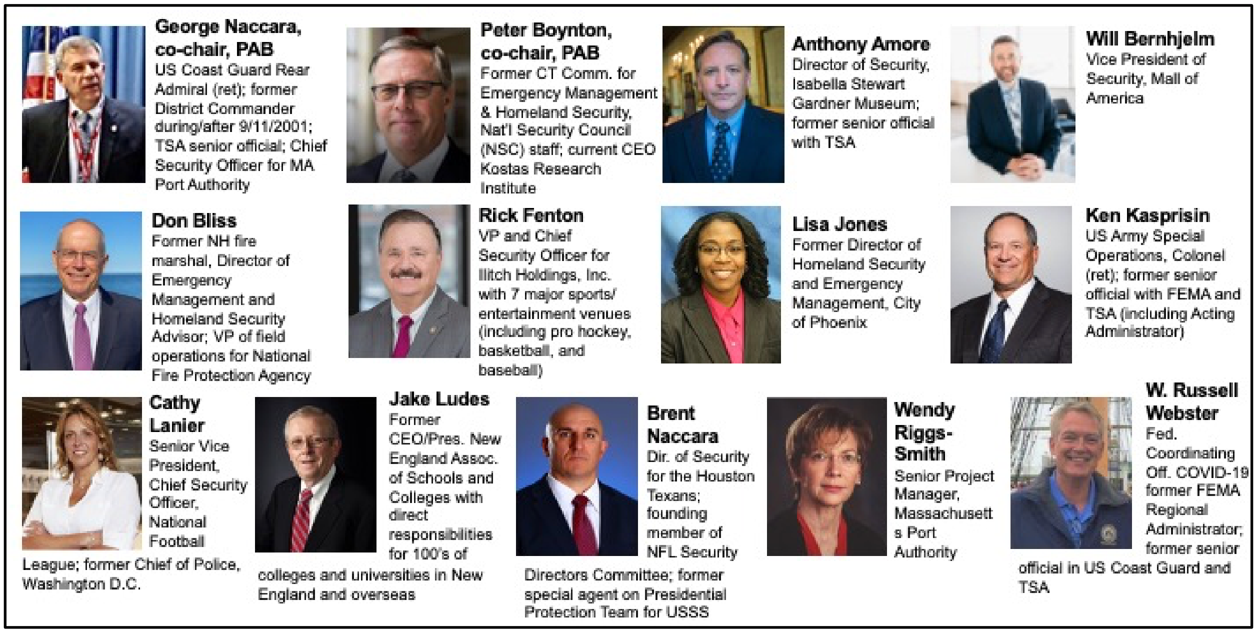
Members of the Executive Committee have large-scale technical leadership expertise of their own, including:

- David Castañón, Deputy Director of Gordon-CenSSIS, Associate Director of ALERT, former member of Air Force Office of Scientific Research (AFOSR) Scientific Advisory Board
- Midge Cozzens, Education Director of CCICADA DHS COE, Board of Directors of the Consortium on Mathematics and its Application
- Emel Bulat, ALERT industrial liaison, former Director of Emerging Technologies at Textron Systems

- Jun Zhuang, PI of 30+ research grants funded by the NSF, DHS, Department of Energy, AFOSR, and the National Fire Protection Association

D. Policy-Practitioner and Industrial Advisory Boards

The Policy-Practitioner Advisory Board (PAB) and Industrial Advisory Board (IAB) will guide SENTRY activities from complementary perspectives. Members include world-class experts in the specific challenges of STCPs and representatives from leading commercial firms in this sector. They will participate in COE routine and large-scale events as appropriate, as well as in the formal evaluation process described in Section 7.2. **Figures 7-2 and 7-3** show the current composition of the PAB and IAB, respectively.



George Naccara, co-chair, PAB US Coast Guard Rear Admiral (ret); former District Commander during/after 9/11/2001; TSA senior official; Chief Security Officer for MA Port Authority

Peter Boynton, co-chair, PAB Former CT Comm. for Emergency Management & Homeland Security, Nat'l Security Council (NSC) staff; current CEO Kostas Research Institute

Anthony Amore Director of Security, Isabella Stewart Gardner Museum; former senior official with TSA

Will Bernhjelm Vice President of Security, Mall of America

Don Bliss Former NH fire marshal, Director of Emergency Management and Homeland Security Advisor; VP of field operations for National Fire Protection Agency

Rick Fenton VP and Chief Security Officer for Ilitch Holdings, Inc. with 7 major sports/ entertainment venues (including pro hockey, basketball, and baseball)

Lisa Jones Former Director of Homeland Security and Emergency Management, City of Phoenix

Ken Kasprisin US Army Special Operations, Colonel (ret); former senior official with FEMA and TSA (including Acting Administrator)

Cathy Lanier Senior Vice President, Chief Security Officer, National Football League; former Chief of Police, Washington D.C.

Jake Ludes Former CEO/Pres. New England Assoc. of Schools and Colleges with direct responsibilities for 100's of colleges and universities in New England and overseas

Brent Naccara Dir. of Security for the Houston Texans; founding member of NFL Security Directors Committee; former special agent on Presidential Protection Team for USSS

Wendy Riggs-Smith Senior Project Manager, Massachusetts Port Authority

W. Russell Webster Fed. Coordinating Off. COVID-19 former FEMA Regional Administrator; former senior official in US Coast Guard and TSA

Figure 7-2. The SENTRY Policy-Practitioner Advisory Board (PAB) provides SENTRY with a Deep Understanding of STCP venues.

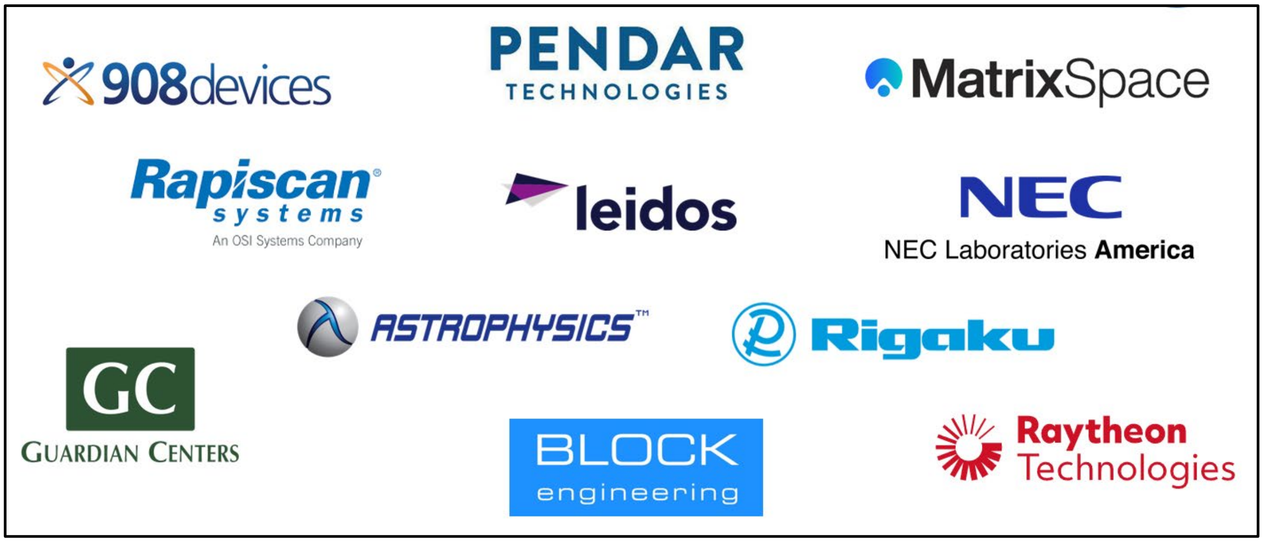


Figure 7-3. The ALERT/SENTRY Industrial Advisory Board (IAB) provides SENTRY with a powerful vehicle for transition of technology into STCP venues.

E. Administrative Staff

Name	Area of Responsibility
Deanna Beirne	IT & Transition
Kristin Hicks	Workforce & Prof. Development; Program Operations
Anne Magrath	Finance & Contracts
Tiffany Lam	Communications & Events
Desiree Linson	Industrial Partnerships
Makenna Lorange	Data & Reporting

Table 7-1*. Administrative Staff and Responsibilities*

Table 7-1 lists the key staff members who will contribute to the SENTRY mission. This efficient and experienced staff is necessary to carry out administrative tasks such as general center management, event planning, scheduling, financial accounting, monitoring and tracking grants and contracts administration, information exchange, communications, reporting and evaluation, and IT support. The staff will set up and maintain contact information and records to ensure proper communications with program participants. The staff will also facilitate communication with partnering institutions and industry and government partners.

7.2 RESEARCH AND PROGRAM EVALUATION

The technical challenges outlined in the SENTRY Program are significant and will require new approaches to overcome the underlying research barriers. In order to effectively accomplish the goals related to research, transition, education and workforce development outcomes, the SENTRY leadership will need to develop a strategic evaluation plan that can assess performance at both the project level and the program level. Effectively managing and evaluating the outcomes of this complex enterprise presents a challenge nearly equal to the basic research challenges themselves. To support this effort, the SENTRY leadership understands that each functional area within the Center must maintain its own unique charter, while considering evaluation methods that will have the necessary rigor, transparency and credibility to provide a relevant and useful assessment of progress towards and accountability for desired outcomes. In this section, we first discuss the SENTRY overall program evaluation, followed by a discussion of the more detailed processes for evaluating the SENTRY research projects, workforce and professional development projects and their respective transition outcomes. Both the program and project-level evaluation plans are needed to ensure continued relevance of the COE to the DHS mission.

A. Program Evaluation

The SENTRY leadership team (identified in Section 7.1) will be actively engaged in the ongoing assessment of research, transition and workforce and professional development (WPD) for both existing and potential new partnerships. Existing programmatic efforts in those three key areas will be evaluated as part of a cyclical review process. Input is solicited for this review from both DHS and thrust leaders, while ultimate responsibility for funding decisions lies with the Director. In addition to these key center efforts, strategic administrative functions – including communications, financial management, and outreach – will be evaluated by the Executive Committee and the Director.

SENTRY has an over-arching Strategic Plan based on the three-level structure shown on **Figure 1-2**. This plan will be augmented by the specification of short- and long-term goals for each SENTRY research, WPD projects as well as for the transition elements. Each project will have associated metrics that will be used to evaluate progress, and these goals and metrics will form the basis for reporting and presentation materials submitted in the yearly or biennial DHS evaluation cycle. Evaluation of the communications, financial management and outreach program elements of SENTRY will also be performed. Examples of metrics that could be used by research, transition and WPD efforts alike include: a) which groups from the Homeland Security Enterprise (HSE) is the project interacting with, and what have been the outputs or results of those interactions in a given year, and b) what have students done after graduation, including how many have moved into the HSE. Examples of metrics for communications and outreach include: a) how often has SENTRY work been reported in the media, and b) what the quantifiable audiences are that have been reached through those reports. Fiscal management can be measured by a) the number and frequency of incoming invoices from the partners and b) the timely reporting of expenditures to the DHS Program and Contracting Officers.

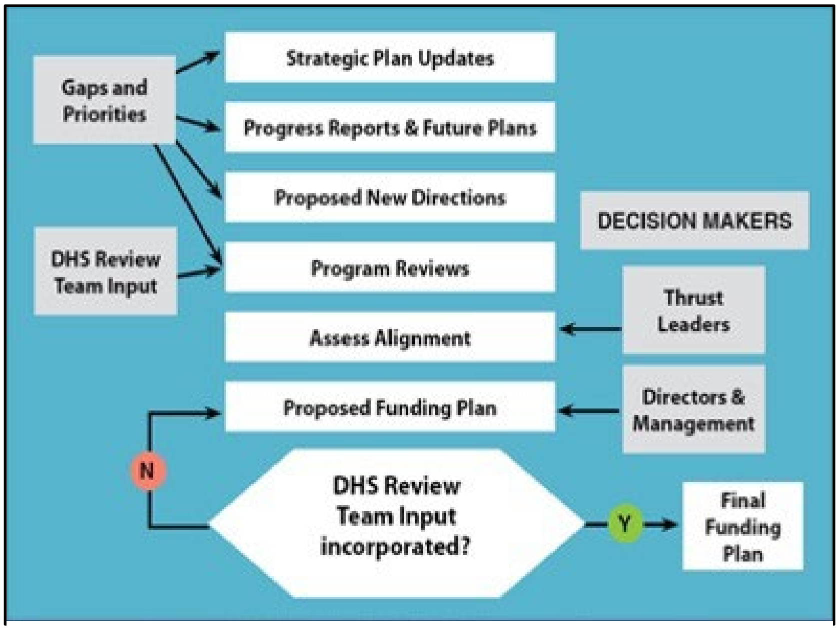


Figure 7-4. The SENTRY biennial program evaluation process keeps the COE focused on its goals and mission.

Figure 7-4 shows the elements of the biennial program review process, which shows how the biennial funding plan evolves after the biennial review. Pragmatically, some research and Workforce and Professional Development Program (WPDP) projects will be terminated and new ones solicited via a competitive process. A formal Call for Proposals will be developed and disseminated through SENTRY communication channels (as identified in Section 7.1) to solicit new project proposals. The Executive Committee will conduct a proposal review process with certain review criteria identified in the Call for Proposals. The Center Director will review the result of the Executive Committee review with the DHS Program Manager and ultimately decide on new projects to add to the SENTRY portfolio.

B. Project Evaluation

The thrust leaders from the Research, Transition and Workforce and WPDP domains have the primary interaction with the individual project leaders and staff. As such, they will provide the first level of evaluation. The thrust leader has immediate oversight of his/her research program; requests for reports coming from management or requests for publication coming from PIs will go through the thrust leader. This allows the thrust leader to continually monitor the technical quality of the projects while maintaining active communication between the project investigators. There are various opportunities to showcase SENTRY throughout the year, so it is expected that the thrust leaders will present their programs in a cohesive fashion. In doing so, thrust leaders can evaluate the success or failure of each project, link successful programs, and disseminate research data to the interested government or industry partners. Not only does this ensure integration of projects, but it also pinpoints areas of weakness or lack of relevance.

The Transition Team Leaders interact with individual projects in an effort to assist them in meeting their established transition goals. This requires a quarterly review process at which the project leads and the transition team work together to discuss project developments and opportunities to advance the project through the transition stage-gate process (identified in Section 4). Transition reviews will consider the projects Technology Readiness Level (TRL) and determine if the research is ready for laboratory, testbed or component-based testing and evaluation. Feedback from these reviews will be provided to the respective thrust leads for inclusion in their overall evaluation of each project. The quarterly assessments of each research project will be given to the project PIs, the thrust lead and the Director/Deputy Director. Each project will receive feedback on continuous improvement. If it becomes clear, after several quarters, that a project is not meeting its milestones then, following concurrence from the DHS Program Officer, the project will be terminated at the end of a given fiscal year.

WPDP leads will oversee the WPDP projects using the specific stage-gate process described in Section 3. While each of the WPD projects targets a different aspect of the DHS and HSE workforce pipeline, they all are expected to provide results that can be documented, such as increasing numbers of students involved in internships or graduates involved in HSE careers, dissemination of course modules to increasing numbers of community colleges and increased numbers of students learning about disciplines related to protection of STCPs. If WPDP projects are not showing evidence of impacts, they will need to be adapted or replaced in the same way that underperforming research projects need to document deficiencies and needed improvements. For WPDP projects that are terminated, a process similar to the research Call for Proposals will be instituted.

DHS requires annual reports and many intermittent calls for data or outcomes over a given year. Meeting these reporting deadlines gives the thrust leaders and the Director insight into weak or lagging program areas.

7.3 SUMMARY

In summary, this Section deals with the management and evaluation infrastructure of SENTRY. These two critical aspects of Center operations are key to its long-term success.

Section 8: Budget Information

The approved budget for SENTRY is detailed in the cover page of the Center of Excellence (COE) Cooperative Agreement Terms and Conditions of the Financial Assistance Division (GFAD) provided to SENTRY dated February 17, 2021. Budgetary information for each research and WPDP project was submitted with the official report to DHS but has been redacted for public dissemination in this abridged report. Breakdown of funding by budget category was also submitted with the official report to DHS in Appendix B but has been redacted for public dissemination in this abridged report.

This page intentionally left blank.

Section 9: Data Acquisition & Management Plan (DAMP), Information Protection Plan (IPP), and Research Safety Plan (RSP)

Requirements for the SENTRY Data Acquisition and Management Plan (DAMP), Information Protection Plan (IPP), and Research Safety Plan (RSP) are defined in Article I. A.10 (DAMP), 11 (IPP), and 15 (RSP) of the Center of Excellence (COE) Cooperative Agreement Terms and Conditions of the Financial Assistance Division (GFAD) provided to SENTRY dated February 17, 2021. SENTRY created the following DAMP, IPP and RSP in compliance with these requirements.

SENTRY Administration will be reviewing all of these plans with SENTRY Thrust Leads and Researchers in the fall of 2022.

These plans are found in Appendix C.

This page intentionally left blank.

Section 10: Conclusion

The SENTRY Center of Excellence has established a strong strategic base, supported by both a meaningful vision and a mission that integrates research and education. In this first year, the Center has launched its initial research and WPDP projects. Because of the late start date, some of these efforts have not had sufficient time to make significant progress. This will not be the case in Year 2. Strategically, however, SENTRY has augmented its research portfolio with the incorporation of case studies. These efforts, starting with school safety, will enable the COE to move concretely toward the design and implementation of Virtual Sentry (VS) systems.

The Safety Program as well as the Information and Data Management Programs have been established. The Policy-Practitioner Advisory Board (PAB) has been active and has provided strategic guidance toward the definition and implementation of the case studies. Industrial members have been recruited and have formed the Industrial Advisory Board (IAB). SENTRY has also continued the ADSA Workshop series started by the ALERT COE, thus creating collaborative opportunities by engaging participants from industry, national labs, vendors, government, and academia in an integrated setting where the Center acts as a “neutral broker.” This is vital in the further development of a dynamic network that can foster the innovative basic research, education, and technology transition needed to help DHS in its mission to safeguard our nation.

In summary, the SENTRY leadership has developed a firm base from which it can quickly adapt to encompass new research and education priorities to address DHS needs. Beyond Year 1 and using the Basic Ordering Agreement vehicle, SENTRY will move forward with its dynamically evolving three-level strategy to advance the state-of-the-art in homeland security technologies. The SENTRY team is proud to be able to help DHS meet the demands of its daunting mission of protecting Soft Targets and Crowded Places.