CREATE
University of Southern California

S&T Analysis and Management of Innovation Activity IV (STAMINA IV)

Benefit Statements, Benefit-Cost-Risk Analysis, and Integration of Key Performance Indicators (KPIs) and Indicators of Success (IoS) into the S&T Business Process Flow (BPF)

Appendix A: Benefits/Impacts Statements – Methodology and Five Applications

FY24 Annual Report
For Period September 29, 2023, to September 28, 2024

September 28, 2024

DHS Science and Technology Directorate (S&T)
Office of Science and Engineering (OSE)
Technology Scouting and Transition Division (TST)

Basic Ordering Agreement (BOA): HSHQDC-17-A-B0004
Contract No. 70RSAT22G00000007
Order No. 70RSAT23FR0000080

Detlof von Winterfeldt, Principal Investigator (PI), Richard John and Isaac Maya, Co-PIs

Project Team: Katie Byrd, Jeffrey Countryman, Susan Chavez, Aleyeh Roknaldin, and Kaitlyn Werden

Center for Risk and Economic Analysis of Threats and Emergencies (CREATE)
University of Southern California (USC)
1150 S. Olive St., 17th Floor
Los Angeles, CA 90015

This research was supported in whole or in part with Federal funds from the US Department of Homeland Security (DHS) through the Center for Risk and Economic Analysis of Threats and Emergencies (CREATE) at the University of Southern California (USC) under Basic Ordering Agreement HSHQDC-17-A-B0004 / 70RSAT22G00000007 / 70RSAT23FR0000080. This report does not necessarily reflect the views or policies of DHS, nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government. Furthermore, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of DHS, or USC, or CREATE.

CREATE
University of Southern California

S&T Analysis and Management of Innovation Activity IV (STAMINA IV)
FY24 Annual Report for Period September 29, 2023 to September 28, 2024

Appendix A: Benefits/Impacts Statements – Methodology and Five Applications

The S&T Analysis and Management of Innovation Activity IV (STAMINA IV) project consists of a Base Period from September 29, 2023, to September 28, 2024, and a 12-month Extension. This Appendix provides the results of Task 1, which includes the following sub-tasks and schedule.

TASK	DESCRIPTION	MILESTONE	SCHEDULE
1.1	Examine a range of transitioned knowledge and technology products	Review of transitioned projects and preliminary benefits statement	12/31/23
1.2	Develop a method for conducting analysis supporting the development of benefits statements and inputs to BCA	Report on benefits statements and inputs to BCA	3/31/24
1.3	Apply the method to a mixed sample of at least ten representatives of previously reported knowledge and technology products	Ten applications and summary report	6/30/24
1.4	Revise the method based on Task 1.3 and develop a Guide	Method refinement and guide	7/31/24
1.5	Train S&T Transition Managers on the methodology	Training workshop	9/25/24

Table of Contents

Appendix A: Benefits/Impacts Statements – Methodology and Five Applications

A1. Simplified Benefits Statement Methodology

- **Description of the KTP (starting with the current tables of 179 KTPs)**
  - Title
  - Short description
  - Developer, program manager or POC, customer
- **Baseline Description**
  - Description of the task, operation, or policy that the T&KP addresses
  - Description of the baseline (including level of effort, baseline impacts/benefits, if available)
- **KTP Transition Impacts/Benefits**
  - Choice of one or more benefit categories from CREATE's list of 10+ categories (the "10" stands for CREATE's monetizable benefits, the + stands for the nine monetizable benefits)
  - Description of how the KTP improves on the baseline in terms of the selected benefit categories
  - Additional co-benefits of the KTP not on CREATE's list
- **Likelihood of a Successful Transition and Implementation for Eventual Use**
  - If a KTP has not yet been transitioned, description of its level of maturity (e.g., TRL or similar)
  - Any other information bearing on transition risks (e.g., current customer involvement)
- **Key Indicators of Performance and Indicators of Success**
  - KPIs: Data required to determine Costs and Benefits
  - IoS: Estimated net benefits based on calculations using the KPIs

A2. Benefits Categories

Benefits Categories (monetized)

- CS: Reduced cost of operations without reducing performance.
- PI: Increased performance without increasing cost
- RR(T) Reduction of threats
- RR(V) Reduction of vulnerabilities
- RR(C) Reduction of consequences
- SDT(D) Increased detection rates
- SDT(F) Reduced false alarm rates
- VOI: Value of information to reduce uncertainty
- VOI: Value of Information to improve operations and decision making
- VoT: Value of Training

Benefits Categories (non-monetized)

- Filling gaps in an integrated technology system
- Satisfying legislative or regulatory requirements
- Responding to Congressional inquiries
- Supporting appropriations requests

- Supporting prioritization of DHS activities
- Improving emergency management
- Improving coordination between agencies
- Other impacts and benefits

A3. Detection Canine Program

Description of the Project

- Title: Detection Canine Program

- Short Description of the Project
    - The detection canine program has partnered with DHS partners, including TSA, and industry stakeholders to bring focus to the domestic detection canine supply challenge through FY 2021. The program established a breeding roadmap, which TSA endorsed. The program concept was validated by a Congressionally mandated Breeding Working Group comprised of S&T, TSA, academia and industry representatives. The working group validated a construct integrating the best scientific practices in genetics, genomics, breeding, olfaction, behavior, training, physiology, and metrology. The program provides tools/knowledge, including odor chemistry expertise, breakthrough laboratory analysis capabilities, specialized T&E experts, and canine operations and training expertise to improve operational proficiency of DHS and HSE canine teams.

- Developer, Program Manager, and Customer
    - Developer: S&T Detection Canine Program
    - Program Manager: Guy Harthough
    - Customer: TSA, Industry

Baseline Description

- Description of the task, operation, or policy that the project addresses
    - Canines are used for explosives detection in airport and other facilities prone to explosive attacks. The TSA, for example, has about 1,000 explosive detection canines in US airports.
    - Prior to the project, TSA staff performed canine breeding, training, and performance evaluation.

KTP Transition Impacts/Benefits

- Two benefit categories from the list of 17 provided by CREATE
    - Reduction of false alarm rates
    - Increase in detection rates
    - Threat reduction

- Description of how the KTP improves performance vs. the baseline
    - Current baseline false alarm rates are <90% and detection rates are 80% to 90% in experimental test evaluations. Actual rates are probably at the low end of these spectra. The canine detection program helps its customers to improve these rates by assisting with breeding, training, and evaluation of canine performance. The program reduces the cost of unproductive time by security personnel and passengers/visitors by reducing false alarms, which can add up to substantial amounts/year. By increasing the detection rate, the program reduces the threat and vulnerability of explosive attacks.

KTP Transition Status

- **Maturity of the KTP:**
    - The program is mature, having been transitioned and implemented for a few years now. The collaboration with the TSA on other parts is in progress. Other customers could also benefit from the program, and efforts are being made to increase participation.

- **Possible transition risks:**
    - There are no risks to this program; the opportunity is to increase participation beyond TSA, thereby increasing the program's benefits substantially.

Key Performance Indicators (KPIs) and Indicators of Success (IoS)

- **KPIs**
    - False alarm rate
    - Detection rate
    - Wait time due to false alarms
    - Costs
- **IoS**
    - Reduced wait time
    - Reduced threats
    - Reduced vulnerabilities

A4. The Water Network Resilience Tool

Description of the Project

- Title: Water Network Resilience Tool

- Short Description of the Project:
    - This project develops an AI-based tool to assist water utility staffers in identifying locations needing resilient pipes in areas of high risks (e.g., earthquakes) and near critical infrastructure assets (e.g., hospitals).

- Developer, Program Manager, and Customer

- Developer: Center for AI in Society, USC (Bistra Dilkina, PI), award from the Critical Infrastructure Resilience Institute (CIRI), an OUP COE
- Program Manager: OUP Program Manager for CIRI, Research Director of CIRI
- Customer: Water Utilities, case study of Los Angeles Department of Water and Power

Baseline Description

- Description of the task, operation, or policy that the project addresses
  - Currently decisions on whether to replace regular pipes with resilient pipes are made manually based on maps of critical infrastructure assets and risks (e.g., proximity to earthquake faults)

- Description of the way the task is performed without the project
  - This task involves many hours of manual work and approximate reasoning about prioritizing resilient pipe needs
  - This may also involve locating resilient pipes in areas of less need and replacing many pipes with resilient pipes at higher costs

KTP Transition Impacts/Benefits

- Two benefit categories from the list of 17 provided by CREATE
  - Risk reduction
  - Cost savings

- Description of how the KTP improves performance vs. the baseline
  - Risk reduction: Reduces the vulnerability of critical assets with properly placed resilient pipes in earthquake-prone areas
  - Cost savings: Reduces time and effort for planning, reduces the cost of unnecessary placement of resilient pipes
  - Additional co-benefits of the KTP: N/A

KTP Transition Status

- **Maturity of the KTP:**
  - The project is close to being used by the customer; the likelihood of successful use is 0.90. The project has been under development for several years and is in its last year of transition. Work is done closely with one customer.

- **Possible transition risks:**
  - Requires sensitive data about locations of critical assets
  - Requires significant participation by the customer to provide data

Key Performance Indicators (KPIs) and Indicators of Success (IoS)

- **KPIs**

  - Cost of resilient pipe replacement prior to WNRT
  - Cost of resilient pipe replacement prior with WNRT

- **IoS**
  - Reduced material cost of resilient-type replacement

A5. FREYJA Cybersecurity Software Tool

Description of the Project

- Title: FREYJA: Uninterpreted functions

- Short Description of the Project:
  - This project develops a software tool intended to provide the Cybersecurity and Infrastructure Security Agency (CISA) of DHS with capabilities to automate threat prediction, malware recognition, identification, and mitigation. FREYJA is part of the Vanaheimr suite of six tools (also including AEGIR, SIGYN, MINISBRUNNER, ODINN, and SKADI) that contribute to CISA's Threat-Focused Reverse Engineering (TFRE) project.

- Developer, Program Manager and Customer

  - Developer: Sandia National Laboratories (SNL)
  - Program Manager: Sean Harris (as of May 2023)
  - PI: Jina Lee (as of May 2023)
  - Customer: Main end users are the malware analysts at CISA/Threat Hunt; future end users include analysts at CISA/Vulnerability Management

Baseline Description

- Description of the task, operation, or policy that the project addresses
  - Currently, it takes malware analysts one week to extract indicators of compromise (IoC) of a binary

- Description of the way the task is performed without the project
  - Manual tools are used to extract indicators of compromise and reveal malware behaviors

KTP Transition Impacts/Benefits

- Two benefit categories from the list of 17 provided by CREATE
  - Improvement of performance and cost savings
  - Improvement of signal detection rates

- Description of how the KTP improves performance vs. the baseline

- Develops scalable abstractions to see through obfuscation and reveal malware behaviors
- Makes it easier for analysts to extract indicators of compromise and understand malware behaviors at-scale
- Analysts will be able to quickly extract indicators of compromise, resulting in faster and better malware analysis.
- One week reduced to minutes to extract indicators of compromise (IoC)

KTP Transition Status

- Maturity of the KTP
  - Transitioned new methods and software to FRIGG.
  - Previewed to CMA analysts.
  - Delivered specific improvements to CISA/FRIGG, enabling FRIGG to scalably extract indicators of compromise in minutes, which used to take a week.

- Possible transition risks
  - Lack of support for implementation and maintenance: Implementation and maintenance depends on CISA/FRIGG funding

Key Performance Indicators (KPIs) and Indicators of Success (IoS)

- **KPIs**
  - Pre-FREYJA CISA cost (or FTEs) of malware detection
  - Post-FREYJA CISA cost (or FTWs) of malware detection

- **IoS**
  - Reduced cost of malware detection

A6. SIGYN Cybersecurity Software Tool

Description of the Project

- Title: SIGYN: Adversary-inspired Rigorous Resilience

- Short Description of the Project:
  - This project develops a software tool intended to provide the Cybersecurity and Infrastructure Security Agency (CISA) of DHS with capabilities to automate threat prediction, malware recognition, identification, and mitigation. SIGYN is part of the Vanaheimr suite of six tools (also including AEGIR, FREYJA, MINISBRUNNER, ODINN, and SKADI) that contribute to CISA's Threat-Focused Reverse Engineering (TFRE) project.

- Developer, Program Manager and Customer
  - Developer: Sandia National Laboratories (SNL)

- Program Manager: Sean Harris (as of May 2023)
- PI: Jina Lee (as of May 2023)
- Customer: Staff at CISA's Vulnerability organization; the tool can be leveraged by any group using a machine learning model with binary and source code as input (e.g., malware analysts, vulnerability research analysts)

Baseline Description

- Description of the task, operation, or policy that the project addresses
  - Current manual threat prediction, malware recognition, identification, and mitigation take weeks to find vulnerabilities in existing machine learning models

- Description of the way the task is performed without the project
  - Manual ML tools are used to recognize, identify, and mitigate threats and malware

KTP Transition Impacts/Benefits

- Benefit categories from the list of 17 provided by CREATE
  - Risk reduction (Reduction of vulnerabilities and negative consequences)

- Description of how the KTP improves performance vs. the baseline
  - Risk reduction: Uses adversarial machine learning to probe tools for weaknesses and then applies mitigations.
  - The tool reduces the time needed to find vulnerabilities in existing machine learning models from weeks to minutes.
  - End users are any team developing a machine learning model that inputs binaries or source code.

KTP Transition Status

- Maturity of the KTP
  - Project is estimated to be completed by the end of POP25
  - Applied adversarial attacks on CISA/BIFROST and CISA/MIMIR.
  - Exchanged knowledge gained and lessons-learned to CISA/LOKI, CISA/BIFROST, CISA/MIMIR.
  - Exposed weaknesses of their machine learning models and suggested mitigations.
  - Started implementation of an automated process to integrate counter-adversarial machine learning (CAML) techniques into machine learning development pipelines.

- Possible transition risks
  - Lack of training: Knowledge of how to install and run the tool in the target environment is imperative when using the tool.
  - Lack of maintenance support: Bug fixes and updates of packages are required every 3-6 months.

Key Performance Indicators (KPIs) and Indicators of Success (IoS)

- **KPIs**
  - Time required to detect vulnerabilities and mitigate
  - Annual frequency of cyberattacks
  - Annual cost of cyberattacks

- **IoS**
  - Reduced time to detect vulnerabilities
  - Reduced frequency of cyberattacks
  - Reduced cost of cyberattacks

A7. Shoe Scanner

Description of the Project

- Title: Shoe Scanner for TSA Checkpoints

- Short Description of the Project:
  - Millimeter wave imaging system that can look through the bottom of your shoes and detect concealed threats inside shoes
  - Next-generation, high-definition scanner that can identify even smaller threats with fewer false positives
  - A shoe scan involves the traveler pausing on a low-profile imaging platform for about two seconds
  - Electromagnetic waves are used to generate an image of the shoe, which is evaluated to determine if an object may constitute a threat

- Developer, Program Manager, and Customer
  - Developer: PNNL
  - Program Manager: TBD
  - PI: TBD
  - Customer: TSA

Baseline Description

- Description of the task, operation, or policy that the project addresses
  - Without the show scanner, airline passengers must take off their shoes and place them on the general scanner with laptops and hand luggage. Only TSA-Pre or Clear passengers (about 20%) do not have to take off their shoes.

- Description of the way the task is performed without the project
  - Taking off shoes takes time, exposes the feet to possible contamination, creates delays and may create hazards due to falling

KTP Transition Impacts/Benefits

- Benefit categories from the list of 17 provided by CREATE
  - Time and cost savings
  - Improved detection rates
  - Reduced false alarm rates
  - Reduced risks of falling
  - Reduced risks of contamination

- Description of how the KTP improves performance vs. the baseline (up to 20% time reduction, according to the developer).
  - Reduced time during TSA check points due to avoiding taking off shoes
  - Potentially improved detection and false alarm rates
  - Reduced risks of falls and contamination

KTP Transition Status

- Maturity of the KTP
  - Project had several starts and stops
  - In the early development stage, TSA performance criteria were not met
  - Later cost concerns were raised
  - Still not implemented

- Possible transition risks
  - Cost
  - Performance

Key Performance Indicators (KPIs) and Indicators of Success (IoS)

- **KPIs**
  - Time for using the shoe scanner vs. time for taking off shows, placing them on the regular scanner, and putting them back on
  - False alarm and detection rates
  - Incidents of falls, injuries, and contamination

- **IoS**
  - Time savings and related cost savings
  - Time and cost savings due to reduced false alarms
  - Risk reduction due to improved detection
  - Reduction of health risks