Overview

The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program supports the global cyber risk research community by coordinating and developing real world data and information sharing capabilities – tools, models, and methodologies. In order to accelerate solutions around cyber risk issues and infrastructure security, the IMPACT program enables empirical data and information sharing between and among the global cyber security research and development (R&D) community in academia, industry, and the government.

Background

Cyber security R&D requires real-world data to develop advanced knowledge, test products and technologies, and prove the utility of research in large-scale network environments. Established and funded by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD), the predecessor program --Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) was the only publically-available, legally-collected distributed repository of large-scale datasets containing real network and system traffic to advance state-of-the-art cyber security R&D. It provided the research community access to infrastructure and event data to facilitate and develop tools, test theories, and identify workable solutions against cyber threats.

IMPACT Value Proposition

In April 2016, PREDICT transitions to IMPACT: Information Marketplace for Policy and Analysis of Cyber-risk & Trust, a name meant to reflect an evolved implementation of the program's goals:

- Marketplace - A more open platform to connect and socialize data supply & demand;
- Policy and Analysis - Research infrastructure and analysis driven by and for real world issues; and
- Cyber-risk & Trust - Beyond just "defense" and "threats," information as a critical infrastructure itself; responsible innovation

IMPACT offers a unique, distributed research data repository supported by a streamlined legal framework and centralized coordination of a controlled distribution of datasets. This centralized brokering and distributed provisioning between the data providers, data hosts and researchers addresses the operational, trust and administrative costs and challenges that impede sustainable and scalable data sharing. IMPACT continually adds new data that is responsive to cyber risk management (e.g., attacks and measurements) to provide the R&D community timely, high-value information to enhance research innovation and quality. The IMPACT model also serves as a laboratory for testing various data sharing models, including traditional batch transfers, newer data-as-a-service (DaaS), and visualization techniques.

IMPACT consists of four components supporting core functional requirements for data sharing: metadata discovery, data and tool matchmaking, trusted brokering, and a social feedback loop.
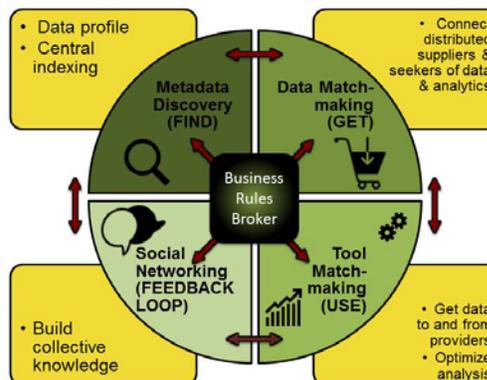
Join us

For more information VISIT DHS- Cyber Security Division or contact us by e-mail.

Homeland Security
Science and Technology

To learn more about the Cyber Security Division's IMPACT Program, contact Erin Kenneally, Program Manager.

2015–08-07