


ENDURING SECURITY FRAMEWORK

A RETROSPECTIVE





The Enduring Security Framework (ESF) was established in 2009 as a cross-sector working group that facilitates collaboration between public and private industries, providing an engagement forum across a broad spectrum of projects that protect critical infrastructure.



PREDICATED ON THE ESSENTIAL NEED FOR COLLABORATION,

the ESF was established to be the premiere forum to address cybersecurity issues facing the nation, government, and industry. Neither government nor industry can do it alone; the reliance on each other fortifies the need for government and industry partnership.



GENERAL PAUL M. NAKASONE
Former DIRNSA



Over the past 15 years, ESF has been a differentiator in leveraging public-private partnerships to address intelligence-driven threats to critical infrastructure. Their ability to unify partnerships in a collaborative forum has led to the release of cybersecurity products that have helped to drive and shape the security of U.S. national security systems and critical infrastructure across the communications, Defense Industrial Base, and information technology sectors.”

GUIDING PRINCIPLES





FOCUSING efforts on high priority cyber-based threats to National Security Systems (NSS) and critical infrastructure;



ADDRESSING key technical issues that pose near-term risk to critical infrastructure in the mission space;



ENSURING a holistic and comprehensive perspective of threats and potential solutions by engaging all relevant stakeholders;



ORGANIZING efforts around mitigating a specific threat or vulnerability;



ACTING with agility to implement change within participating organizations and influencing the broader community to achieve near-term results;



MAINTAINING trust and operational discretion appropriate to protecting sensitive information;



DELIVERING timely technical outputs for actionable implementation; and



ENABLING implementation of outcomes to achieve broad impact.



STRUCTURE



THE ESF IS COMPRISED of three different, but equally important, groups that convene regularly to discuss new and advancing cyber concerns: The Executive Steering Group (ESG), Operations Group, and Working Panels.

These groups align industry and government interests to deliver consensus on strategic, technical, and operational mitigations to cybersecurity risks that impact national security.



The ESG is co-led by the Deputy Secretary of Defense (DepSecDef), Deputy Secretary of Homeland Security, the Director of National Intelligence and participating company Chief Executive Officers. They develop the strategic vision and provide the Operations Group with related objectives to implement that vision.



The Operations Group is led by senior government and industry participants, including the Director of the National Security Agency (NSA), the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and Chief Technology Officers from across the industry. Their focus is on substantive issues with defined outcomes and results. They also oversee the tactical work of the Working Panels.



The Working Panels are topic-specific teams comprised of subject matter experts from public and private industry. The members research security solutions and define recommendations for mitigation.

ESTABLISHMENT



ANNE NEUBERGER
First ESF Chief

The ESF broke new ground in showing what was possible in a partnership between the public and private sectors. Across chipset, software, and hardware, millions of laptops, computers, and servers were protected against an imminent threat. This initial spark began a partnership that utilizes a cooperative model for identifying relevant constituencies and how they can best serve each other.”

THE ESF LETTER OF INTENT,

penned by the Department of Defense (DoD), Department of Homeland Security (DHS), and Office of the Director of National Intelligence (ODNI), pledged sponsorship and oversight of ESF.



OCT 2008

Due to growing the Committee on Foreign Investment in the United States concerns and informal industry roundtables hosted by DepSecDef England, NSA was tasked to collaborate with DHS to establish and charter ESF as a cross-sector working group.

JAN 2009

First ESG hosted by DepSecDef.



MAR 2016

Leveraged modern network architectures and big-data analytics for insider threat attack detection.

JUN 2011

Devised a plan to mitigate an emerging class of threats targeting core computer system firmware.

MAY 2021

5G Threat Vectors
First publicly attributed ESF product that addressed vulnerable 5G vectors.

AUG 2013

Developed guidance and security requirements to minimize effects of destructive malware through increased resiliency of information and communication systems.

SEP 2022

Software Supply Series
Provided guidance to NIST for safeguarding the software development cycle.



"We can turn your computer into a brick."

"Cyber Briefings 'Scare The Bejeezus' Out of CEOs"
May 2012, NPR Morning Edition

DEC 2023

OSS/SBOM
Compiled and published best practices for OSS/SBOM.

GOVERNMENT PARTICIPATION



ALAINA CLARK
IT/Comms GCC Chair

The ESF is made possible through the power of collaboration and public-private partnership. CISA's Critical Infrastructure Partnership Advisory Council authority enables this function and enhances the program's effectiveness, efficiency, and value while also promoting unity among its members. Our partners work closely together to identify technical gaps and implementation challenges, which is essential for securing the nation's critical infrastructure and national security systems."

5G SUCCESSES



FOLLOWING THE RELEASE of the National Strategy to Secure 5G, ESF was tasked with identifying threats and mitigations that affect 5G usage. Over a two-year period, U.S. government and industry partners within ESF collaborated on the development and production of a variety of security products for addressing 5G threats. Many of these were the first USG-produced security products of their type and each made major strides in the advancement of the nation's 5G security.

IMPACTS



HIGH PERFORMANCE COMPUTING (HPC)

OCT 2008–DEC 2009

Examined strategies for sustaining the United States' capability to create state-of-the-art HPC in a globally competitive timeframe.



MOBILITY/MOBILE DEVICE INTEGRITY (MDI)

JUN 2011–APR 2013

Developed architectural requirements to make mobile devices suitable to access enterprise networks and data in a "Bring Your Own Device" scenario. MDI requirements ensure that device integrity, protected storage, and isolation are met.



DDOS/ DESTRUCTIVE MALWARE

FEB 2012–OCT 2012

Accelerated implementation of commercial mitigations that improved the security of our corporate and national infrastructure against network-based attacks.



RISK MANAGEMENT OF OUTSOURCED NETWORK SERVICES

DEC 2015–DEC 2018

Developed an assessment tool which allows organizations to make risk-informed decisions when outsourcing network services.



BIOS

SEP 2010–JUN 2011

Developed requirements for securing client and server BIOS. Addressed platform security, including protection of PC option ROMs and BIOS on network devices. Developed firmware integrity reporting mechanisms that serve as a fortified defense for a variety of platforms.

IMPACTS

CYBER RESILIENCY AGAINST DESTRUCTIVE MALWARE

(AUG 2013-SEP 2016)

Developed detailed guidance and security requirements to minimize effects of destructive malware through increased resiliency of information and communication technology systems, including the ability to withstand and rapidly recover from intrusions.



COMMERCIAL THREATS/ YARA SUB-TEAM

MAR 2017–DEC 2019

Determined how public and private sectors could work together to address high-risk circumstances associated with software, product, and virtualized service vendors in the global ICT supply chain.



RESILIENT TIME IMPACT

SEP 2017–DEC 2019

Developed guidance for advanced awareness of resilient time and time hygiene as a critical component of cybersecurity.



5G THREAT VECTORS

MAY 2021

First publicly attributed ESF product that addressed vulnerable 5G vectors.



OSS/SBOM

DEC 2023

Compiled and published best practices for OSS/SBOM.

INDUSTRY PARTICIPATION



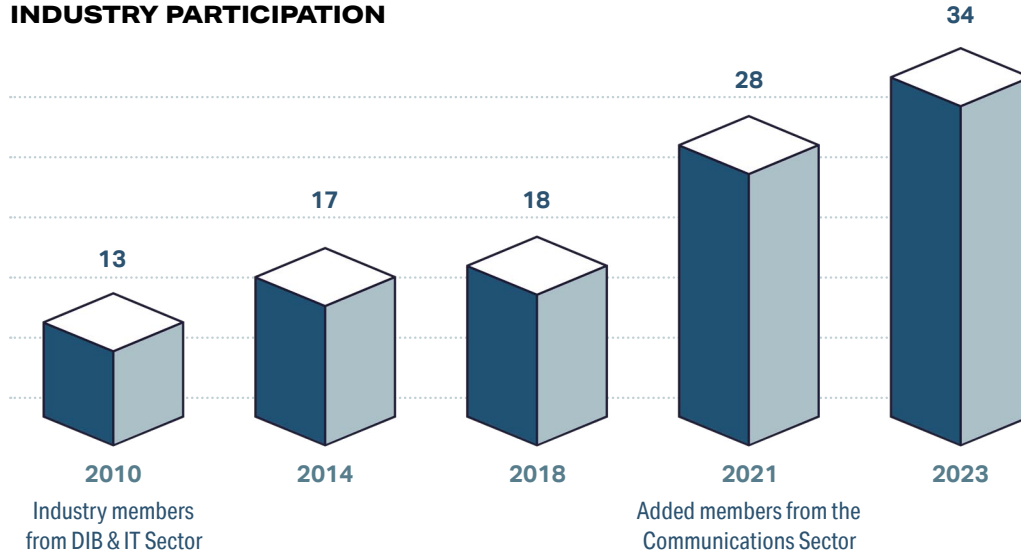
MIKE GORDON

Chair, DIB SCC



ESF joined DoD and DHS with key companies in the Defense Industrial Base (DIB) and in two other sectors in a unique collaboration to secure the national interests of the United States...ESF has afforded DIB companies key insights about critical technical challenges facing the United States, but also the chance to help shape the solutions. The relationships and processes created over the last 15 years will be essential to tackle the challenges in the next 15 years."

INDUSTRY PARTICIPATION



SINCE ITS INCEPTION, the ESF has been an effective forum to develop defensive cybersecurity solutions. Industry participation in ESF has almost tripled with the Communications critical infrastructure sector joining ESF in 2021. The success of ESF has only been possible through growing public/private partnerships, exchanging threat intelligence, face-to-face collaborations, and cooperative writing and editing of technical mitigations and best practices.

FUTURE



THE ESF HAS PROVEN

that public-private partnerships get results. For years we have achieved success amid evolving technology, increasingly sophisticated threats, complex coordination for solution implementation, and global events.



INTERNATIONAL STANDARDS

Examining and providing recommendations to help achieve increased participation in standards bodies which is vital to national security systems for the U.S. and its allies.



EDGE COMPUTING

Assessing edge computing vulnerabilities and their associated threats, identifying potential threat vectors and areas of greatest impact to critical infrastructure.





As we prepare for new focus areas and fresh challenges for the ESF to address and overcome, we continue to maintain the spirit of collaboration at the highest levels of government and industry that has made us stronger together and fostered cyber preservation for all.

CYBERSECURITY
POWERED THROUGH



PUBLIC-PRIVATE
PARTNERSHIP



NSAESF@cyber.nsa.gov