Huntington Ingalls Industries
Hard Stuff Done Right™

We deliver solutions
with resilient
cyber foundations
at their core

CYBERSECURITY SOLUTIONS

Go Beyond Compliance for a Mature Cybersecurity Posture

The United States' public and private sectors are at continual risk from both nation-state and non-state cyber threat actors, with no sign of lessening ahead. Amid today's complex, volatile threat environment, it's not hyperbole to suggest that cybersecurity must be a top priority for every national defense and intelligence leader.

A CONNECTED DEFENSE MUST BE SECURE

In response to these threats, the government has instituted a number of programs and policies to help secure the nation's systems, including guidance found in the Risk Management Framework from the National Institute of Standards and Technology (NIST), which offers standards and best practices to manage cyber risk across operations.

While these practices are essential, they don't necessarily allow an organization to keep pace with cyber threats as they evolve. With advances in artificial intelligence (Ai) and deep learning, defense and security operators are now able to predict threats before they appear. By incorporating Ai-based threat prevention, the U.S. can move beyond compliance to a position of true cybersecurity maturity.

COUNTER THE THREATS AS THEY EVOLVE

With 25 years of experience developing innovative cybersecurity solutions, our experts understand today's threats and how to counter them. We deliver solutions with resilient cybersecurity at their core, using applied Ai for complete vulnerability analysis and adaptive systems that learn how to fend off attacks.

At Huntington Ingalls Industries (HII), we go beyond consulting to apply practical cyber solutions for our clients. And we deliver these solutions securely via engineers who all maintain a full cybersecurity workforce certification in their respective domains. In fact, our secure solutions are assessed by independent validators, authorized by DoD Authorizing Officials (AO), and stand up to the tough scrutiny imposed by cybersecurity inspection teams across the DoD.

As the U.S. wages cyber battles of the future, we are poised to help identify, mitigate, and counter the changing threats at whatever rate they evolve. Together, we help clients protect their networks, assets, and missions all around the globe.

HII'S CYBERSECURITY SOLUTIONS

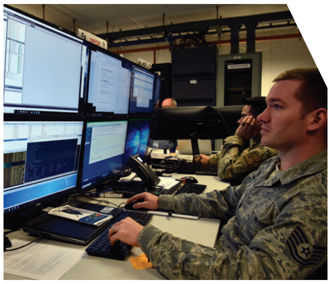
We are deeply analytical partners who never stop looking for a way to make things better. That's why we apply our vendor-agnostic approach and agile engineering methodology to every project, saving our clients time and money while delivering industry-leading cybersecurity solutions. Protecting the people who dedicate their lives to defending us is at the heart of everything we do.

ENTERPRISE CYBERSECURITY

HII engineers build and secure a wide range of enterprise technology solutions specialized for defense or national security environments and approved by DoD Authorizing Officials.

THREAT & ATTACK MODELING

We use real-time, low-cost, behavior-based enterprise cybersecurity tools to perform DoD protocol inspections while seamlessly integrating cyber into distributed environments.



EMBEDDED CYBER TOOLS

Pulling from our strengths in embedded system design, we offer a suite of hardware-based, cyber-resilient technologies, resulting in processing platforms that are hardened by design.

ASSESSMENT & AUTHORIZATION

We conduct thorough threat analysis and select discrete mitigating controls to provide secure, resilient solutions and attain DoD Authorities to Operate (ATO) for our clients.

SPOTLIGHT ON: CYBER MATURITY ASSESSMENTS

We successfully defined an end-to-end process for conducting Assessment and Authorization (A&A) for the Navy Continuous Training Environment (NCTE), a secure, globally-distributed enterprise network that spans 47 Commands at 147 locations, interconnecting with 23 training partner networks.

Using the NIST Risk Management Framework (RMF) as a baseline, this process addresses each of the six steps in RMF and includes a series of quality assurance checkpoints. Our approach goes beyond mere compliance with the requirements to also point out key areas for cybersecurity maturity, such as configuration, change management, and best practices for network/IT deployment and lifecycle— providing a more holistic risk picture of the organization.

HII was the first contractor organization to achieve an Authorization to Operate (ATO) using RMF for the Navy Authorizing Official (NAO) and has since achieved five full Navy RMF ATO's using our unique process. We also partnered with the NAO to help develop the Navy's RMF process and have been lauded by USFF as the standard for Navy RMF.

We help clients maintain reliable, secure, and useful network and physical environments with the tools and support they need to run a smooth operation. To learn more about our complete package of cybersecurity solutions, or to connect with one of our experts, visit us online at tsd.huntingtoningalls.com.

CONTACT:
John Eubank
Vice President
Cyber & Electronic Warfare
john.eubank@hii-tsd.com
443.717.2100

About Huntington Ingalls Industries, Technical Solutions:
Building on a legacy of more than a century of naval shipbuilding, Huntington Ingalls Industries' Technical Solutions division provides mission-critical national security solutions to a wide variety of government and commercial customers worldwide. Comprising more than 7,000 professionals worldwide, our unique national security services portfolio includes unmanned systems, nuclear and environmental services, intelligence, surveillance and reconnaissance (ISR), cyber and electronic warfare, live, virtual and constructive (LVC) training solutions, and fleet sustainment and logistics. For more information, visit tsd.huntingtoningalls.com.

Huntington Ingalls Industries
Hard Stuff Done Right™
tsd.huntingtoningalls.com