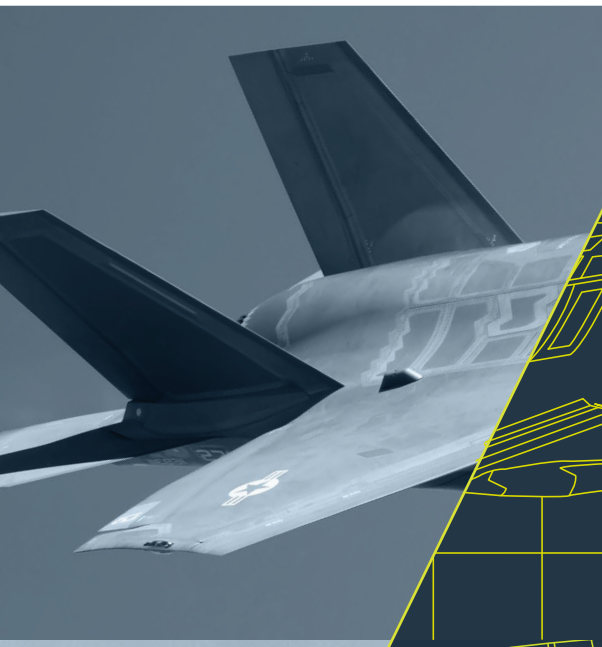
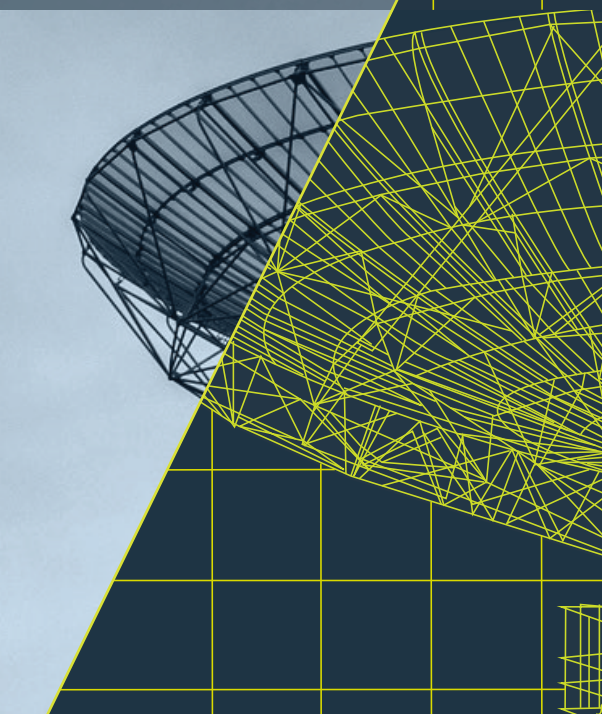
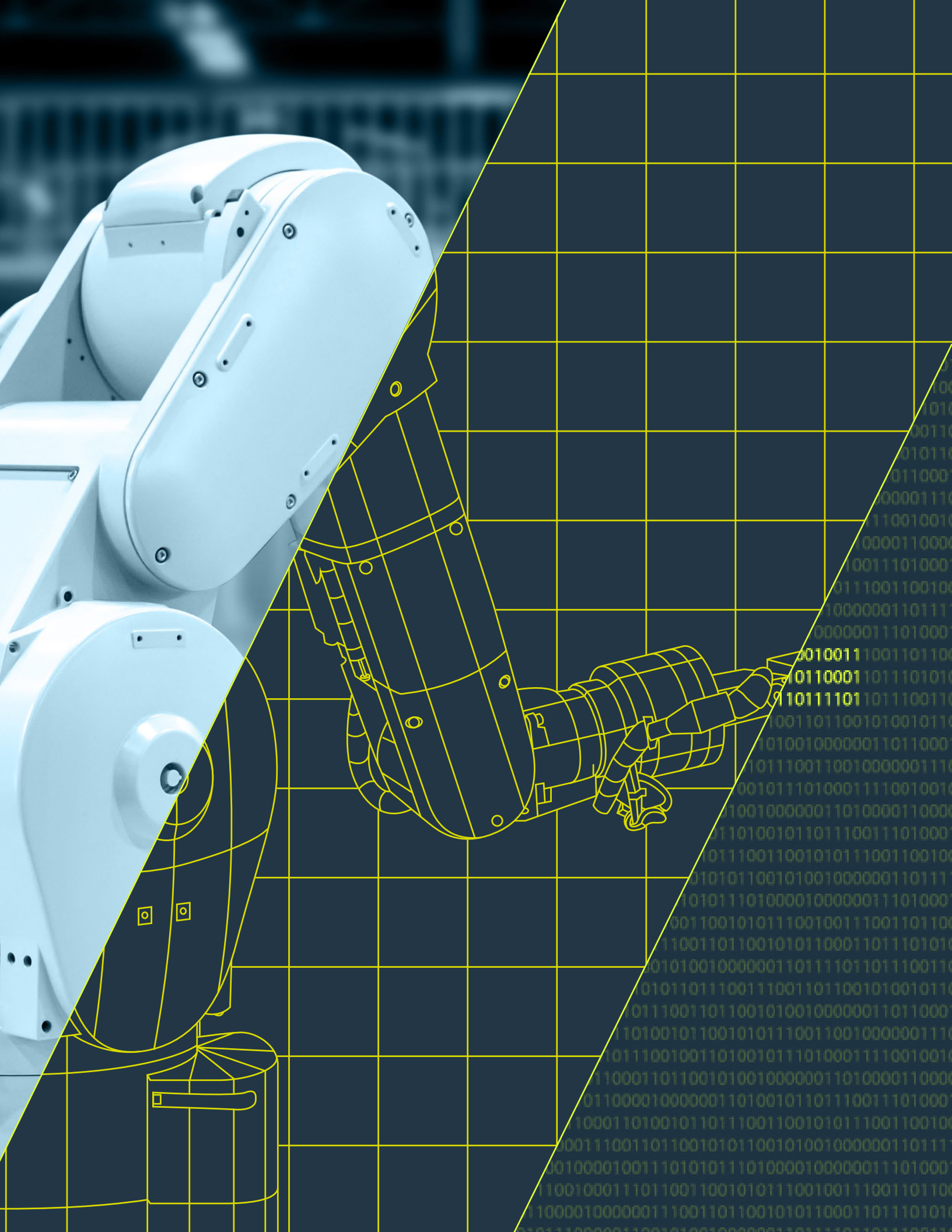
HOW TO SUSTAIN U.S. CYBER SUPERIORITY

HARNESS COLLABORATION, INNOVATION, OFFENSE, AND DEFENSE





Booz Allen®



Tomorrow's cyber threats will likely eclipse yesterday's. That's why the 2022 National Security Strategy calls for decisive action to protect vital national functions and critical infrastructure—and it's why the National Cybersecurity Strategy doubles down on disrupting and dismantling threat activities. To prevail and outpace adversaries, the United States must now employ cyber offense and defense in a seamless manner. What's needed is not just security and resilience, but also cyber superiority.

Neither nations nor organizations can afford to wait for a catastrophic cyber event to improve their defenses. But not even the best cyber defense programs guarantee protection against determined adversaries. Nor can redlines safeguard critical infrastructure. Cyber conflict is being waged in the shadows—but the danger is clear enough. Digital cloak-and-dagger operations, fueled by rising geopolitical tensions, threaten to undermine trusted IT systems, connected devices, and operational technology (OT), potentially causing physical effects.

Adversaries view the federal government, intelligence agencies, the military, and all critical infrastructure industries as one large target-rich environment—one cyber battlespace. To gain the advantage, the United States, allies, partners, and the private sector must create unity of effort. This requires urgent progress on three fronts: fostering operational collaboration, focusing innovation, and integrating cyber offense and defense capabilities with other tools of national power to deter and counter threats.

NEITHER NATIONS NOR ORGANIZATIONS CAN AFFORD TO WAIT FOR A CATASTROPHIC CYBER EVENT TO IMPROVE THEIR DEFENSES.

6 DAYS

The duration of the Colonial Pipeline shutdown in the 2021 ransomware incident

Source:
Department of Energy

$10 BILLION

The estimated global economic damage from the 2017 NotPetya cyberattack

Source:
Wired

$193 BILLION

The cost of a global ransomware attack in a severe hypothetical scenario

Source:
Lloyd's

TOP 5 RISK

How cyberattacks on critical infrastructure rank among 2023 global risk perceptions

Source:
World Economic Forum

SIGNS OF PROGRESS— AND KEY OBSTACLES

FOSTERING OPERATIONAL COLLABORATION

PROGRESS

Operational collaboration is about building and leveraging trusted partnerships between government and industry to elevate national cybersecurity through collective action. Stakeholders in government and industry have been striving to achieve this ideal for years. Early information-sharing success stories like responses to threats from **Hidden Cobra and Cozy Bear** have been succeeded by the achievements of CISA's **Joint Cyber Defense Collaborative (JCDC)**, which aims to unify cyber defenders worldwide, and the National Security Agency's (NSA) **Cybersecurity Collaboration Center (CCC)**, which focuses on protecting the defense industrial base and sensitive government systems. When the Log4j vulnerability came to light in 2021, the JCDC enabled rapid sharing of indicators of compromise, threat activity, and intelligence. And in 2022, the CCC nearly tripled its partnerships to harden almost 2 billion endpoints against nation-state threats. Further, CISA has shown resolve by prioritizing operational collaboration in its **strategic plan**.

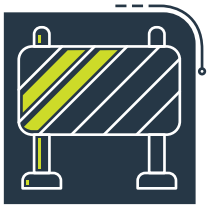
OBSTACLES

Much work remains to be done across the public and private sectors to strengthen ties and build trust. It's been nearly a decade since the Obama administration issued an executive order on cybersecurity information sharing to spur the creation of cross-sector sharing hubs, and since Congress passed the Cybersecurity Information Sharing Act of 2015 with liability protections for industry. But the essence of the challenge has not changed. Critical infrastructure companies are still seeking more timely and actionable cyber threat intelligence and insights from the government, while the government remains concerned that companies are not sharing enough information about the cyber threats targeting private-sector data, networks, and operations. Businesses must trust that sharing information with the government will improve collective cyber defense, not trigger penalties, and the government needs to provide greater assurances to that effect. Achieving operational collaboration will require breaking down barriers across the people, process, and technology dimensions of cybersecurity and questioning longstanding assumptions about information sharing. Agencies should focus on identifying and understanding impediments and defining pathways to overcome them.

FOCUSING INNOVATION WHERE IT'S NEEDED MOST

PROGRESS

Innovation is easy to lionize in principle but hard to tame in practice. The White House has **committed** to increasing investment and expediting technology development in cybersecurity and other industries in the future. Also, the Defense Advanced Research Projects Agency (DARPA) is playing a key role in coordinating the development of innovative cyber capabilities for both offense and defense. The expanded collaboration between DARPA and U.S. Cyber Command (CYBERCOM) in the new **Constellation program** holds great promise. The program is all about accelerating the development of new capabilities through rapid prototyping and integration. In addition, the innovation arms of **DOD**, the Department of Homeland Security (**DHS**), and **CISA** are all partnering with industry to develop cyber solutions.



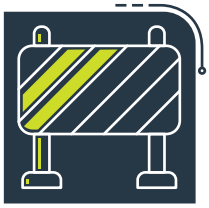
OBSTACLES

For organizations looking to outpace threats, acquiring truly novel solutions is a real challenge. Even the U.S. government's commitment to cybersecurity is no guarantor the latest innovations will be put in place where and when they are needed most. Beset by buzzwords and vendor hype, federal agencies spend billions of dollars chasing shiny objects that seldom produce measurable security improvements for vital missions. The government should make targeted investments in leading cyber capabilities, safeguard the technology, cultivate crucial industrial base elements, and aim to deploy novel solutions that help the government and private sector protect missions and critical infrastructure. Further, stakeholders should apply the concept of innovation more broadly—not only to technology but also to cyber strategies and processes.

INTEGRATING OFFENSE AND DEFENSE

PROGRESS

CYBERCOM marked a key milestone in 2022: With the consent of Ukraine, the Cyber National Mission Force (CNMF) deployed its largest-ever hunt forward team. The team hunted for malicious cyber activity on Ukrainian networks, working alongside Ukrainian cyber experts. The effort enabled disruption of malicious activity before it could cause harm. In addition, insights and adversarial tools and capabilities "were shared with U.S. domestic interagency and public/private industry partners to improve U.S. homeland cyber defenses," **according to the command**. This is a major step in the right direction.



OBSTACLES

Defensive and offensive operational planning functions across federal, intelligence, and defense agencies are too often siloed in terms of missions, resources, and capabilities. This creates uneven cyber defensive readiness where some agencies are less capable and knowledgeable when dealing with advanced adversaries. What's more, this disconnect makes it harder for the owners of offensive cyber missions to benefit from data and insights generated during defensive operations and to leverage best-in-class solutions for their offensive missions.

WHAT'S NEXT:
STEPS TO TAKE NOW

Widespread cyber insecurity is one of the **top global risks** in the near term and for the next decade. Here are steps that leaders can take now to build security, resilience, and cyber superiority:

FOSTERING OPERATIONAL COLLABORATION

- The public and private sectors must focus on achieving tangible outcomes. Although there is a need for some regulation, stakeholders must guard against sacrificing agility and effectiveness on the altar of bureaucracy. To protect the nation's most important critical infrastructure, the majority of which is owned and operated by the private sector, the Biden administration is expected to use its National Cybersecurity Strategy to make the case for expanded regulatory authorities. In doing so, the administration must ensure that emerging regulation does not undermine industry's willingness to participate in cybersecurity information-sharing processes and partnerships.
- The government and the private sector should collaboratively develop an approach that ensures both the public and private sectors gain significant value from sharing threat data and insights. Trust is so difficult to achieve—both sides must give to get this right.
- CISA and the NSA could significantly strengthen progress by rapidly reaching a consensus on a collaborative environment for sharing cyber threat information among government and industry stakeholders. Report language tied to the Fiscal Year 2023 National Defense Authorization Act calls for a study on how best to implement the idea, which originated with the U.S. Cyberspace Solarium Commission. It will not be easy, but this is an opportunity to create unity of effort.

FOCUSING INNOVATION

- DHS should leverage the Homeland Security Advisory Council's **study** on building a more robust "Homeland Security Technology and Innovation Network" to find new opportunities to support the development of novel cybersecurity solutions for critical infrastructure.
- DOD should support national cybersecurity with its forthcoming National Defense Science and Technology (S&T) Strategy. "Cyber" is in the name of just one of **14 critical technology areas of focus**. But many other listed areas—quantum science, future-generation wireless technology, and trusted artificial intelligence, for starters—tie in with national cybersecurity. Opportunities to advance cyber defense and offense with S&T should be top of mind as DOD crafts S&T priorities—and as the Defense Innovation Board performs its related **independent assessment**. DOD should also seek to continue advancing cyber innovations through **strategic investment capital**.
- DARPA and CYBERCOM's **Constellation program** and related efforts to develop leading tools for cyber offense and defense should be well resourced by Congress over the long term. This program is likely to equip the U.S. with essential tools for carrying out the policy of integrated deterrence, a vital element of the National Security Strategy and the National Defense Strategy. Any progress in capability development might also ultimately enable better integration of offensive and defensive operations.
- As discussed at the 2022 **Cyber Beacon** event hosted by the College of Information and Cyberspace (CIC) at National Defense University (NDU), DOD should do more protect the thin sliver of the U.S. industrial base that possesses world-class expertise researching zero-day vulnerabilities. When tapping researchers to reliably

develop zero-days for intelligence and military missions, the U.S. government should prioritize working with U.S. firms. Also, the U.S. should provide more counterintelligence support to these researchers, who are being targeted by foreign spies.

- Agencies and companies should adopt leading strategies such **data-driven cybersecurity** and **zero trust**. For the latter, organizations should start by using a zero trust assessment framework to identify areas where improvement is most needed. Along the way, organizations lagging in cybersecurity fundamentals must be brought up to par.

INTEGRATING OFFENSE AND DEFENSE

- The U.S. should continue the dual-hatted arrangement in which CYBERCOM and NSA are led by the same four-star general. In addition, the nation should leverage this arrangement's inherent speed and agility, as well as the CNMF's recently elevated importance as a **subordinate unified command**, to further advance the integration of offense and defense.
- The nation should plan, fund, and create a dedicated **cyber intelligence center** at CYBERCOM to focus on foreign cyber forces and extremist groups and provide intelligence support to both defensive and offensive cyber operations. Over time, this center could also help attract and grow cyber talent to meet long-term needs.
- Leaders should strengthen the sharing of cyber intelligence and insights across the federal government to better inform U.S. analysts and operators and pursue expanded operational collaboration with critical infrastructure sectors that enables synchronization.
- The government should increasingly leverage national-level cybersecurity exercises and wargames to stress test synchronization efforts, including in crisis response scenarios.
- The U.S. should integrate offensive and defensive cyber capabilities with other tools of national power to deter and counter hostile cyber activities.
- The U.S. should work closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve cyber resilience, and to build collective capabilities to rapidly respond to attacks.

The future of national cybersecurity depends on a unified approach to protect what adversaries see as one cyber battlespace. It depends on operational collaboration, innovation, and the integration of offense and defense. Most importantly, it depends on you and your organization. The steps taken today to build U.S. cyber superiority will make all the difference tomorrow.

LEARN MORE AT BOOZALLEN.COM/NATIONALCYBER

EMPOWER PEOPLE TO CHANGE THE WORLD®

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital solutions, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision.

With global headquarters in McLean, Virginia, our firm employs approximately 29,500 people globally as of March 31, 2022, and had revenue of $8.4 billion for the 12 months that ended on March 31, 2022. To learn more, visit www.boozallen.com. (NYSE: BAH)