Cyber Risk Management and Prioritization

SPONSORING ORGANIZATION
National Security Agency (NSA)

CHALLENGE
The NSA Defense Industrial Base (DIB) cybersecurity team needs a standardized evaluation of the cybersecurity risk posed by defense companies working with the government in order to prioritize mitigation methods to prevent cybersecurity incidents.

RELEVANT CONTEXT
- Currently, DOD is looking to evaluate over 100,000 DIB companies as part of their cybersecurity risk strategy. Due to the large workload, NSA's DIB cybersecurity team who has been tasked to oversee the evaluation needs to first identify partners who present the greatest cybersecurity threat.
- The NSA is already conducting small-scale cyber security-as-a-service pilots for DIB companies and is looking to scale these services.
- While there is public research about the cyber risk posed by individuals, less is known about the business risk posed by companies not in the insurance industry. There is currently no standardized evaluation of business cybersecurity risk.

IMPACT
A solution to this problem will allow the DOD and the NSA to prioritize developing mitigation tactics for companies posing the highest cybersecurity risk. This will also ensure that small business government contractors can better understand NSA and DoD cybersecurity practices.

POTENTIAL BENEFICIARIES
NSA Cybersecurity Directorate, NSA Cyber Collaboration Center, NSA DIB Cybersecurity Team, Defense Industrial Base companies

TEAM RECOMMENDED SKILLSETS
Cybersecurity, operations, risk management

RESOURCES
- Statement by REAR ADMIRAL WILLIAM CHASE, DEPUTY PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE May 18, 2021
- U.S. Defense Contractors Failing to Meet CMMC Requirements, 48% Have "Severe" Vulnerabilities July 6, 2021
- "The focus of this report is on the activities of UNC2630 against U.S. Defense Industrial Base (DIB) networks…." April 20, 2021
- Industry matters when assessing cyber risk to the defense industrial base