# New Cybersecurity Framework Aims at Protecting Nation's Critical Infrastructure

IBM

ARMONK, NY – IBM announced a new service offering to help critical infrastructure organizations utilize a new Cybersecurity Framework announced by the Administration at the White House. The new Cybersecurity Framework is the product of a year-long collaboration between the U.S. government and industry, coordinated and led by the National Institute of Standards and Technology (NIST). The goal of the Framework is to help organizations assess and manage cybersecurity risk with respect to key categories and functions, leveraging existing best practices. Today's factories, power facilities and other physical assets are increasingly interconnected, making the Framework strategically important to the security of today's enterprises and the infrastructure they depend upon.

Rather than dictate specific technologies, measures or outcomes, the framework establishes a common language for organizations to evaluate their cybersecurity posture and to identify and prioritize opportunities to improve it. Because the Framework is designed to be adaptable to organizations of different types and sizes, it can be customized to an individual organization depending on its risk profile, resources, and needs.

The IBM Industrial Controls Cybersecurity Consulting service is designed to help companies apply the Framework to baseline and improve their security maturity, prioritize security investments and resources, and protect themselves from cyber risks to infrastructure and elements necessary for critical operations and networks. IBM security consultants will educate clients on details and mechanics of the NIST Cybersecurity Framework and perform a comprehensive assessment of a client's security maturity relative to the guidelines, best practices and international standards referenced in the Framework. Clients receive recommendations for improvements as well as a roadmap for improving capabilities and reducing risk.

"Cyber threats are not limited to select industries such as financial services and retail companies. There is a growing need to apply advanced security to our increasingly interconnected critical infrastructure like power facilities, electrical grids, industrial manufacturing operations and others," said Kris Lovejoy, general manager of IBM Security Services. "If organizations take the steps outlined in the Framework, they'll be better positioned to protect themselves and their practices. IBM can help its clients adopt these best practices now — and to distinguish themselves as an industry leader in security."

The industries most dependent on the nation's infrastructure are also some of the most attacked, according to IBM's own analysis, based on findings in the most recent IBM Cyber Security Intelligence Index [1], security intelligence analysis generated from IBM's global security monitoring operation of over 4000 clients. Data from the report shows that infrastructure-dependent industries are among the most targeted by cyber attackers. The top five industries that reported the most incidents include:

- Manufacturing – 26.5% of all observed security incidents
- Finance and Insurance – 20.9%
- Information and Communication – 18.7%
- Health and Social Services – 7.3%
- Retail and wholesale – 6.6%



**Links:**
[1] http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html