PRESIDENTIAL POLICY DIRECTIVE/PPD-21
Critical Infrastructure Security and Resilience

POTUS EXECUTIVE ORDER (EO)
Improving Critical Infrastructure (CI) Cybersecurity

BACKGROUND, PURPOSE & COAST GUARD ROLE

- PPD-21 cancels HSPD-7 and updates the national approach to protecting CI. It defines CI broadly, to include cyber and other systems as well as physical structures. PPD 21 also expands the view of CI threats from the previous terrorism perspective to an all hazards approach. PPD 21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure across the spectrum of prevention, protection, mitigation, response, and recovery.

- The POTUS Cyber Security EO directs various agencies to assess cyber risks to CI, collaborate on developing best practices, share threat information, and take other action to address cyber risks. The National Institute of Standards and Technology (NIST) has the lead for identifying best practices and developing a "framework" for cyber security while DHS has the lead for identifying and evaluating CI risks. Once the framework is established, DHS will encourage owners of CI to voluntarily adopt the framework

- Various Coast Guard Headquarters staff elements have formed a working group and Executive Steering Committee to implement the requirements of the Executive Order. This group will work closely with DHS, DOT, TSA, and other agencies as part of this effort. The Coast Guard's specific role is as the maritime subsector (Sector Specific Agency or SSA) to the Transportation Sector.

- At the National Level, the Coast Guard will consult with the National Maritime Security Advisory Committee and similar organizations to gain a better understanding of cyber risks in the maritime sector, and to gain advice on how to address those risks.

- At the local level, Federal Maritime Security Coordinators will consult with Area Maritime Security Committees on how to best assess and address cyber risks in the port.

- Forthcoming Strategic Planning Guidance will encourage Coast Guard field commanders to consider cyber in evaluating risks, COOP planning, and in ensuring they are complying with existing direction concerning AIS security and protection of Coast Guard information systems.

WHAT DOES THIS MEAN FOR THE PRIVATE SECTOR?

- ❑ Neither the EO nor PPD 21 sets regulatory requirements for the private sector or creates new authorities for doing so.

- ❑ The Coast Guard has no cyber related rulemaking in progress. The Coast Guard will keep industry informed should new legislation or other action require the Coast Guard to address cyber risks through regulation.

- ❑ Information sharing with the private sector is a key requirement of the EO. It specifically states that U.S. Government policy is "to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." DHS and other agencies have various specific responsibilities under this provision. The Coast Guard has always shared as much information as possible with industry, and we will continue to do so under this EO.

- ❑ The EO states that in developing the cyber security framework, the government "shall engage in an open public review and comment process" and consult with owners and operators of critical infrastructure. The Coast Guard will keep maritime industry and other stakeholders informed about this process as it develops.

- ❑ The private sector should be proactive in evaluating, identifying and mitigating cyber security vulnerabilities. Under the Department of Homeland Security, the United States Computer Emergency Readiness Team (US-CERT) provides a number of tools and services that can improve cyber security, encourages companies and organizations to report incidents and invites the public to join the Industrial Control Systems Joint Working Group. For more information, see http://www.us-cert.gov/.

- ❑ Vessel and Facility Security Plan holders may wish to consider incorporating cyber events into their required security exercises. Please share any insights or lessons learned with your local Captain of the Port.

- ❑ Participate in Area Maritime Security Committee activities, discuss cyber concerns with Coast Guard vessel and facility inspectors, and monitor Homeport for new information. The Coast Guard has established a cyber section of Homeport, https://homeport.uscg.mil, go to Missions > Maritime Security > Cybersecurity. CG CYBERCOM also has information under Library, Publications, Maritime Security "Weekly Cyber Feed".

PPD-21 can be found at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The Executive Order can be found at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity