Critical Infrastructure

Current and future trends and challenges.	*R: Boeing is concerned threat actors are increasingly capable of conducting cyber security attacks with the purpose of achieving disruption to aviation industry critical infrastructure business operations and manufacturing processes for a variety of motivations, in addition to theft of critical intellectual property and other proprietary information. Additionally, Boeing is incurring greater risk from access to government provided data and networks such as weather and positioning data than ever before.*
Progress being made to address the challenges.	*R: Boeing is extending IT Enterprise protections and vulnerability responses to the factory floor and ground operations in addition to enterprise support.*
Most promising approaches to addressing the challenges.	*R: Boeing has formed its own Information Sharing and Analysis Center as well as a new Emerging Vulnerability Response Plan under the Boeing Cybersecurity Community of Excellence as means to address these issues.*
What can or should be done now or within the next 1–2 years to better address the challenges.	*R: Extend DHS and IC efforts to advise and warn critical infrastructure companies and organizations on threats that research methods or seek to conduct attacks for the purpose of disruption to critical infrastructures and services. Predictive trend data may be helpful.*
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	*R: The growing list of countries that harbor or look the other way to indigenous cybersecurity criminal activities must be addressed.*

Cybersecurity Insurance

Current and future trends and challenges.	*R: Boeing is concerned the aviation industry is assuming greater risks and potential for liability as cybersecurity threats continue increase.*
Progress being made to address the challenges.	*R: Boeing is investing in a series of Use Case Studies and Product Development improvement activities to drive down risks and development mitigation plans. These efforts have been recognized by the DHS Safety Act office as best practices towards the identification and mitigation of new risks.*
Most promising approaches to addressing the challenges.	*R: Boeing recommends conducting detailed Use Case Studies and Tabletop Exercises as a means to identify and establish mitigations for new risks.*
What can or should be done now or within the next 1–2 years to better address the challenges.	*R: Boeing has begun to apply its Use Case Study and tabletop exercise method to new critical infrastructure systems during the design/feasibility stage to anticipate and design solutions for potential cybersecurity risks.*
What should be done over the next decade to better address the challenges; and	*R: Implement US and International laws to reduce direct indemnity of critical infrastructure organizations to cybersecurity threats as new normal.*
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	*R: Same as #5 above.*

Cybersecurity Research and Development

Current and future trends and challenges.	*R: Boeing sees many new positive commercial and academic research efforts that may prove useful for the aviation industry.*
Progress being made to address the challenges.	*R: Boeing sees progress being made, but not in coordinated way to bring best of industry R&D approaches to cybersecurity challenges in the aviation and adjacent industries.*
Most promising approaches to addressing the challenges.	*R: Approaches that address machine speed responses, automated detection, rapid risk characterization, predictive, and resiliency.*
What can or should be done now or within the next 1–2 years to better address the challenges.	*R: Private industry and government needs a better means to evaluate emerging technologies across a broad array of implementation and threat scenarios.*
What should be done over the next decade to better address the challenges; and	*R; Government and industry need to work together to prioritize needs and address research and development shortfalls to bring best of government and industry solutions forward.*

Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	*R: Government and industry must be prepared to rapidly integrate breakthrough technologies and techniques across multiple critical infrastructure sectors.*

Cyber Workforce

Current and future trends and challenges.	*R. Boeing, likely many other organizations must train and retain the best and brightest for cyber security. Among other challenges, Boeing has identified promoting a Cybersecurity Culture as one of its priorities for the 2016-2018 timeframe.*
Progress being made to address the challenges.	*R: The formation of the Boeing Cyber Security Community of Excellence and has allowed for better interaction between cyber security functional experts.*
Most promising approaches to addressing the challenges.	*R: Boeing is using a Facebook-like application to facilitate information sharing and crowd source solutions to cyber security challenges of mutual concern across the company.*
What can or should be done now or within the next 1–2 years to better address the challenges.	*R: Better role based training and simulation systems are urgently needed for aviation workforce cyber security development.*
What should be done over the next decade to better address the challenges; and	*R: Conduct comprehensive workforce training that facilitates actions taken at many levels and across critical infrastructure sectors.*
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	*R; We must continue to create greater awareness in the workforce on emerging threat techniques and best practices in risk mitigation across sectors.*

Federal Governance

Current and future trends and challenges.	*R: Boeing, like many other large companies, must report and coordinate its cyber security information sharing and reporting activities across several critical infrastructures (Transportation, Communications, Defense, Critical Manufacturing, etc.) and experiences daily challenges in differences between Sector Specific Agencies in cybersecurity coordination and reporting while maintaining government regulatory compliance requirements (such as; FAA, and Security and Exchange Commission). Often we find these agencies competing for information and at cross purposes in terms of protecting versus disclosing information.*
Progress being made to address the challenges.	*R: The increase in cybersecurity collaboration and information sharing has been helpful, however progress is hindered by an*

	increasingly complex cyber policy landscape within the U.S. Government
Most promising approaches to addressing the challenges.	*R: Government-wide implementation of better standardized indicator and incident reporting templates (e.g. STIX/TAXII) and better information sharing across government organizations.*
What can or should be done now or within the next 1–2 years to better address the challenges.	*R: Require all government agencies to consolidate to common set of cybersecurity reporting and information sharing standards. Also recommend NIST consolidate current government risk management approaches into a single approved standard.*
What should be done over the next decade to better address the challenges; and	*R; Establish a single government organization with all cyber security information sharing and reporting responsibilities for the US Government and oversight over all other government organizations for cybersecurity policies and procedures.*
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	*R; Boeing is already seeing foreign governments establish their own cyber security operational standards and reporting restrictions that may stand in direct conflict with US government cybersecurity reporting compliance requirements.*

Identity and Access Management

Current and future trends and challenges.	*R: Aviation is seeing much greater use of wired and wireless remote access and adoption of next generation mobile devices pervade the industry.*
Progress being made to address the challenges.	*R: Aviation ISAC has recognized the significance of these issues for the aviation industry, which are also addressed in the AIAA Cyber Security Framework (2014).*
Most promising approaches to addressing the challenges.	*R; The recent moves to impose new Supply Chain cyber security software and hardware quality standards and conformance checks for all devices and networks connecting to industry airplanes and business operations systems.*
What can or should be done now or within the next 1–2 years to better address the challenges.	
What should be done over the next decade to better address the challenges; and	
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	

International Markets

Current and future trends and challenges.	*R; Boeing is seeing several foreign governments establish their own cyber security operational standards and reporting restrictions that may stand in direct conflict with US government cybersecurity reporting compliance requirements*
Progress being made to address the challenges.	
Most promising approaches to addressing the challenges.	
What can or should be done now or within the next 1–2 years to better address the challenges.	
What should be done over the next decade to better address the challenges; and	
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	

Internet of Things

Current and future trends and challenges.	*R: Role-based cybersecurity awareness and training, as well as availability of patches and updates for legacy programs are driving factors for improving protections for Internet of Things*
Progress being made to address the challenges.	*R: The Critical Manufacturing Sector Specific Plan addresses cyber security challenges to industry directly in the latest updated plan.*
Most promising approaches to addressing the challenges.	
What can or should be done now or within the next 1–2 years to better address the challenges.	
What should be done over the next decade to better address the challenges; and	
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take	

to best position themselves today to meet those challenges.	

Public Awareness and Education

Current and future trends and challenges.	*R; Aviation industry members and customers must become better aware of cyber security threats and techniques, and we must establish and promote a more proactive cyber security culture across aviation.*
Progress being made to address the challenges.	
Most promising approaches to addressing the challenges.	
What can or should be done now or within the next 1–2 years to better address the challenges.	
What should be done over the next decade to better address the challenges; and	
Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.	

The Commission also seeks input on the following:

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.	*R; Boeing is considering making better use of large data mining, artificial intelligence, and machine speed learning and responses to advance cyber security protections for the aviation industry.*
2. Economic and other incentives for enhancing cybersecurity.	*R; We must ensure continued support for Import-Export Bank as a means to facilitate and ensure the most advanced cybersecurity features for new airplanes are integrated into fleets worldwide.*

3. Government-private sector coordination and cooperation on cybersecurity.	*R; Boeing is currently responsible to report and coordinate its cyber security information sharing and reporting activities across several critical infrastructures (Transportation, Communications, Defense, Critical Manufacturing, etc.) and experiences daily challenges in differences between Sector Specific Agencies in cybersecurity coordination and reporting while maintaining government regulatory compliance requirements (such as; FAA, and Security and Exchange Commission). Often we find these agencies competing for information and at cross purposes in terms of protecting versus disclosing information.*
4. The role(s) of the government in enhancing cybersecurity for the private sector.	*R; Recommend establishing a single government organization with all cyber security information sharing and reporting responsibilities for the US Government and oversight over all other government organizations for cybersecurity-related policies, regulatory requirements, and procedures.*
5. Performance measures for national level cybersecurity policies; and related near-term and long-term goals.	*R: Government should adopt a cross critical infrastructure process for conducting proactive risk management and whole of government-industry (loss frequency vs. loss impact) analysis.*
6. Complexity of cybersecurity terminology and potential approaches.	*R; The cyber security industry is currently plagued with multiple researcher and security advisory organizations using multiple names for the same techniques and threat actor sets. This urgently needs to be standardized and made common for information sharing and response purposes.*