EXECUTIVE ORDER 13873 RESPONSE

METHODOLOGY FOR ASSESSING THE MOST CRITICAL INFORMATION AND COMMUNICATIONS TECHNOLOGIES AND SERVICES

April 2020

CISA
CYBER+INFRASTRUCTURE

This page is intentionally left blank.

KEY FINDINGS

- The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) identified 61 Information and Communication Technology (ICT) elements organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles.
- The 11 sub-roles are:
  - Broadcast Networks
  - Wireless Local Area Networks
  - Mobile Networks
  - Satellite Access Points
  - Cable Access Points
  - Wireline Access Points
  - Core Networking Systems
  - Long and Short Haul Networks
  - Storage and Cloud Based Services
  - End User and Edge Networking Equipment
  - Security and Operations

Contents

Figures

Tables

BACKGROUND

On May 15, 2019, the President signed Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO addresses the threat posed by the unrestricted acquisition or use of Information and Communications Technology (ICT) and services "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," and declares a national emergency with respect to this threat.

The EO requires the Secretary of the Department of Homeland Security (DHS) to produce a written assessment within 80 days and annually thereafter that would "assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States."[1] The assessment "shall include an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers, including the communications services relied upon by critical infrastructure entities identified pursuant to Section 9 of Executive Order 13636."

Within DHS, the responsibility to execute the assessment was assigned to CISA/NRMC on behalf of the Secretary. In its response to this EO, the NRMC coordinated with federal and private partners to assess what ICT hardware, software, and services (referred to individually in this report as elements) present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences.

SCOPE

Information technology and communications technology intersects almost every aspect of operations essential to national security, the Nation's critical infrastructure, and National Critical Functions (NCFs). NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. DHS, through coordination with federal and industry partners, scoped its response to the Executive Order to accomplish the following:

- Develop a taxonomy of ICT elements based on Information Technology (IT) and Communication roles and sub-roles.[i]
- Assess the criticality of ICT element classes based on their sub-role and in the context of the IT or Communications sector function it supports.

This paper describes DHS's methodology for assessing ICT element criticality.

Caveats and Limitations

NRMC faced several challenges in responding to the EO including:

- Conducting a broad assessment with a short timeline that also allows a reasonable amount of time for vetting and validation with industry subject matter experts (SMEs), sector specific agencies (SSAs), and coordinating councils.
- Providing a general assessment of ICT element criticality independent from the application of the element in any specific network or system.[ii]
- Assessing an element known to support critical functions in some systems and non-critical functions in other contexts.

[i] In its response to the EO, DHS is assessing classes of elements rather than makes, models, and versions of elements, but will be able to use these assessments to assess specific makes, models, and versions within the most critical classes of elements in future iterations of analysis.

[ii] A system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- Identifying existing system-specific security measures that mitigate potentially risky attributes of technologies acquired through the supply chain.
- Handling technology trends geared to enable remote access, monitoring, administration, and control.

DHS will work to minimize and address these limitations as it develops its annual assessment as required by Executive Order 13873, as well as augment its assessments with additional analysis.

METHODOLOGY OVERVIEW

With support from Argonne National Laboratory and Sandia National Laboratories, DHS developed a two- step approach to assessing the criticality of ICT hardware, software, and services (ICT elements) in the IT and Communications sectors.[iii] In step 1, DHS developed an ICT Framework to decompose the basic roles and sub-roles ICT elements provide within the IT and Communications sectors, and then identified the elements that support each sub-role. In step 2, DHS developed and executed a repeatable approach for analyzing the criticality of ICT elements.

Each step of the methodology required extensive contributions from ICT SMEs. NRMC partnered with industry through a government established ICT Supply Chain Risk Management (SCRM) Task Force (ICT SCRM TF) to ensure the perspectives and expertise of critical infrastructure owners and operators could provide acute insight into operations and operational use of ICT. The ICT SCRM TF is a Critical Infrastructure Partnership Advisory Council (CIPAC) Cross Sector Working Group where the respective IT and Communications Sector Coordinating Council Chairs serve as the industry co-chairs. Accordingly, the co-chairs were able to solicit representative members from across the IT and Communications sectors, a majority of which are members of the Task Force, to provide input based on their experience and expertise. Additionally, the TF engaged non-member SMEs as necessary to provide inputs to inform the TF recommendations.

Step 1: Developing an ICT Framework

In step 1, DHS developed an ICT Framework to serve as a generic representation of IT and Communications sector roles and sub-roles, which would then be used to identify and bin ICT elements to draw basic judgements about criticality. The ICT Framework is organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles, shown in figure 1 below.

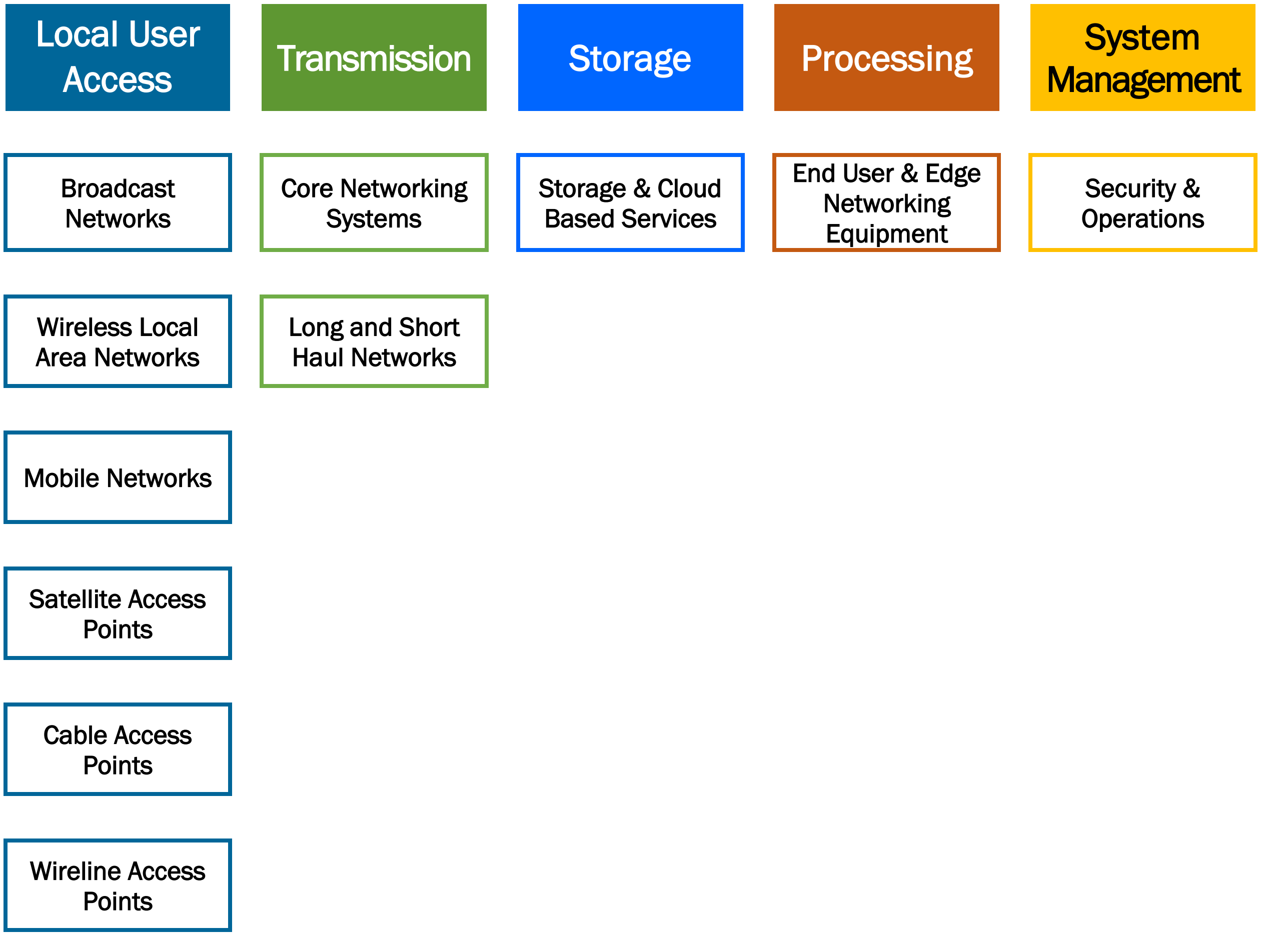
To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. These select NCFs, which align closely with the "Connect" theme, were chosen due to their extensive dependence on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences:

- Operate Core Networks
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

[iii] Due to time limitations, DHS was unable to analyze ICT elements for all critical infrastructure sectors. DHS chose to analyze the IT and Communications sectors because of their criticality for all other sectors.

These NCFs were selected due to their dependence on ICT elements and their criticality for other functions. See Appendix A for more information on NCFs.

When NCFs are decomposed into the ICT elements that support them, each element is organized into the ICT Framework (roles and sub-roles) shown below in figure 1:



Local User Access	Transmission	Storage	Processing	System Management
Broadcast Networks	Core Networking Systems	Storage & Cloud Based Services	End User & Edge Networking Equipment	Security & Operations
Wireless Local Area Networks	Long and Short Haul Networks			
Mobile Networks				
Satellite Access Points				
Cable Access Points				
Wireline Access Points				

FIGURE 1—ICT FRAMEWORK

DHS identified 61 ICT elements (i.e. hardware, software, or services) that support 11 sub-roles of the ICT Framework. The list of 61 elements with definitions is below in table 1.

TABLE 1—ELEMENTS AND DEFINITIONS

ELEMENT	DEFINITION
BROADCAST NETWORKS	
Emergency Alert System (EAS) Encoder/Decoder	EAS encoder/decoders allow TV broadcast stations to take audio signals containing data and filter them for geographic region and emergency event information.
Station to Transmitter Link (STL)	The STL transports program material from a local station's studio to the station's transmitter site for broadcast.

ELEMENT	DEFINITION
Transmitter	A transmitter takes baseband audio, video, or digital signal and converts it to a radio frequency and amplifies it to drive a broadcast transmission antenna.
WIRELESS LOCAL AREA NETWORKS	
Distributed Antenna System (DAS)	A DAS is a network of spatially separated antennas that provide wireless service within a geographic area or structure. DAS will be applicable in Fifth Generation (5G); however, small cells and differing spectrum bands may change how a DAS is utilized.
Small Cells/Micro Cell	A small cell is a miniature base station that transmits short-range radio signals. Due to the limited range and non-penetrative signal of high frequency radio wave bands, 5G will require numerous small cells to support its infrastructure. Together, these cells would form a dense network that relays data through multiple small cells.
MOBILE NETWORKS	
Base Station Controller (BSC)	BSC controls facilitate communication between one or more base stations or cell sites.
Base Station Subsystem (BSS)	In a mobile cellular network, the BSS handles traffic between the cell phone and the network switching subsystem.
Base Transceiver Station (BTS)	A BTS is a 2G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Cell Session Control Function	A system that manages the signaling from end-user to services and other networks, providing the end-to-end connectivity across networks.
eNodeB	An eNodeB is a Fourth Generation (4G) Long-term Evolution (LTE) fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
gNodeB/5G NR	A gNodeB/5G NR is a 5G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
NodeB	A NodeB is a 4G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Home Agent	A router on a home network which enables communication to provider networks.

ELEMENT	DEFINITION
Home Location Register (HLR)	In a mobile cellular network, the HLR is the main database of permanent subscriber Personally Identifiable Information (PII) for a mobile network.
Home Subscriber Server (HSS)	The HSS is the master user database that supports the IP Multimedia Subsystem (IMS) network entities that handle calls and sessions. It contains user profiles, performs authentication and authorization of the user, and can provide information about the physical location of user.
Mobility Management Entity (MME)	The MME is responsible for idle mode user equipment tracking, paging procedure, activation and deactivation process, call handover, and user authentication.
Mobile Switching Center (MSC)	The MSC is the hub that handles many of the communication switching functions, including call setup, routing, release, messaging, and advanced features.
Equipment Identity Register (EIR)	The EIR is a database that contains a record of the all equipment that is allowed in a network and all equipment that is blacklisted.
Policy Decision Function	A ruleset engine that arbitrates the overall features and functions on the network that are available to users, and the allocation of resources and bandwidth available.
Mobile Positioning Center (MPC)	MPC is a service or function that that works to determine the position of a mobile device.
Gateway Mobile Location Center (GMLC)	GMLC is a service or function that that works to determine the position of a mobile device in mobile cellular networks. It is also expected to go away once there is a full conversion to 5G networks.
Media Gateway	A Media Gateway translates media content between various network and communication protocols.
Media Gateway Control Function (MGCF)	An MGCF performs switching and conversion between control switched and packet switched domains, connecting the mobile and standard telephony systems.
Gateway GPRS Support Node (GGSN)	A GGSN provides switching between the General Packet Radio Service (GPRS) network and packet switched networks, and routing on the GPRS mobile network.
Serving GPRS Support Node	A serving GPRS support node provides supporting functions for packet switched data within the network, such as user authentication and management.

ELEMENT	DEFINITION
Session Border Controller (SBC)	SBCs are used by all interconnected Voice over Internet Protocol (VoIP) providers and carriers to establish, maintain, and tear down phone calls through IP based networks.
Operation Support System (OSS)	OSS is comprised of hardware and software systems that allow network operators to perform network monitoring and management functions, such as configuration and provisioning. It also contains a large database of customer information and manages billing information.
SATELLITE ACCESS POINTS	
Satellite Payload	The space-based functional component of the communications platform. The satellite payload is the means by which the satellite mission is accomplished. Example satellite payloads include communications, PNT, signal detection, Overhead Persistent Infrared (OPIR), radar, imaging, etc. The payload may include some of the same component types as the satellite bus (e.g., communications transmitter/receiver, power amplifier, antenna, etc.) and often depends upon the satellite bus for a number of functions including power source, data processing, communication services, etc.
Satellite Bus	The space-craft system hosting the communications payload, which includes satellite navigation components, flight dynamics, fuel tank(s), thrusters, reaction wheels, solar panels, batteries, wiring harnesses, radiation shielding, the frame structures, power distribution, and a basic communication system for receiving instructions called TT&C (telemetry, tracking, and command). The satellite mission will determine the bus design or, conversely, the bus design will constrain the types of missions that can be supported by the satellite. For communications satellites, the payload may be integrated with the communications components of the satellite bus.
Satellite Ground Control Station (SGCS)	Facility providing satellite telemetry, tracking, and command (TT&C) connectivity from the Spacecraft Operations Center to the satellite.
Spacecraft Operations Center (SOC)	Terrestrial-based spacecraft operations facility that maintains the health and safety of the spacecraft and, if applicable, satellite mobility.
Communications Ground Station/Teleport	Ground equipment and facilities for managing subscribers, controlling subscriber access to services, providing billing for services, and providing interoperation between subscriber sessions and other networks.
Satellite Network Operations Center (SNOC)	Provides functionality to maintain network operations, such as providing user access, account management, and network health and operation.
Teleport Network	Terrestrial mesh of multi-terminal ground stations (Teleports) providing bulk space-ground connectivity, as well as interconnecting the various elements of Operations and Gateway Segments.

ELEMENT	DEFINITION
Uplink Facility	Terrestrial-based facility that provides uplink of content to be distributed to subscriber equipment.
CABLE ACCESS POINTS	
Core Server	A core server is a hardware and software system that provides functionality to other devices in the telecommunications backbone or core network, including data, processing, and management services.
Core Router	A core router directs packets through the network, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
Core Switch	A core switch performs packet switching operations, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
WIRELINE ACCESS POINTS	
Access Infrastructure Data Link	An access infrastructure data link is a communications pathway that provides data transmission services to wireline subscribers.
Access Infrastructure Digital Loop	An access infrastructure digital loop provides connectivity from the service provider to wireline subscribers.
CORE NETWORKING SYSTEMS	
Core Infrastructure SONET/SDH	Core Infrastructure SONET/SDH is a widely deployed technology used in implementing high-speed, large-scale Internet Protocol (IP) networks.
Core Infrastructure DWDM/OTN	Core Infrastructure DWDM/OTN are technologies that increase capacity on networks and optimize the existing resources of transportation networks.
Core Infrastructure IP/Internet	Core Infrastructure IP/Internet delivers data from the source host to the destination host within a communication network.
Core Infrastructure CDN Cache	A CDN is a system of distributed servers that deliver web pages and other content to users based on their geographic locations.

ELEMENT	DEFINITION
Core Infrastructure IP/MPLS	IP/Multiprotocol Label Switching (MPLS) refers to a network backbone that uses the IP augmented with MPLS routing. MPLS is a mechanism for routing traffic within a telecommunications network, as data travels from one network node to the next.
Data Center MPLS Routers	MPLS routers that support a data center.
Metro MPLS Routers	MPLS routers that support a metro area.
LONG AND SHORT HAUL NETWORKS	
Fiber Optic Cable	Fiber optic cable is the medium in which transmission of information as light pulses occurs along a glass, plastic strand, or fiber. Fiber optic cable is used across all domains (e.g., enterprise, long and short haul, cable, oceanic, etc.).
Repeaters	A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.
STORAGE AND CLOUD BASED SERVICES	
Server	A server is a hardware and software system that provides functionality to other devices in the system, including data, processing, and management services.
END USER EQUIPMENT & EDGE NETWORKING EQUIPMENT	
LAN Equipment (sensitive)[iv]	Local Area Network Equipment (sensitive) facilitates communication between one or more computers and other devices in a limited geographic area within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
LAN Equipment (non-sensitive)	Local Area Network Equipment (non-sensitive) facilitates communication between one or more computers and other devices in a limited geographic area that is not within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
Mobile Devices (sensitive)	Mobile devices (sensitive) are handheld, portable computing devices that can connect to a cellular network and process classified or sensitive information. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.
Mobile Devices (non-sensitive)	Mobile devices (non-sensitive) are handheld, portable computing devices that can connect to a cellular network and process information that is not classified or sensitive. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.

[iv] An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data's confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

ELEMENT	DEFINITION
Computers (sensitive)	Computers (sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) within a sensitive network or system, or process classified or sensitive data.
Computers (non-sensitive)	Computers (non-sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) and are not located within a sensitive network or system, nor process classified or sensitive data.
SECURITY & OPERATIONS	
Domain Name System (DNS)	DNS translates internet domains and hostnames to IP addresses.
Systems Software (sensitive)	Systems software (sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities, and have been installed on sensitive systems.
Systems Software (non–sensitive)	Systems software (non-sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities and have not been installed on a sensitive system.
Applications Software (sensitive)	Applications software (sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and has been installed on a sensitive system.
Applications Software (non–sensitive)	Application software (non-sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and is not installed on a sensitive system.

Step 2: Assessing Criticality

In step 2, DHS developed and executed a repeatable approach for assessing the criticality of ICT elements. DHS assessed the criticality of each ICT element in the context of the IT or Communications sector function it supports. This enabled DHS to distinguish the criticality of similar elements used in different sub-roles, for example, the difference in the criticality of routers used in core networks responsible for routing terabytes of data as opposed to routers used in home networks for personal use.

DHS worked with SMEs from CISA, industry partners, and national laboratories to collect data to analyze element criticality. Elements were assessed at the following criticality levels:[v]

- **Critical:** Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including

[v] DHS assessed the criticality of element classes based on how their compromise could affect the sub-role they support. With the exception of edge ICT elements (end user equipment, edge networking equipment, and end user software) which DHS assessed based on whether they were used in sensitive or non-sensitive networks, DHS did not identify specific elements that may be more or less critical based on what entities rely on them. For example, an element that supports military functions may be more critical than a similar element that does

affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

- **Manageably Critical:**[vi] Compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.
- **Not Critical:** Compromise of the element is unlikely to have significant regional or national impacts.

DHS assessed the criticality of 61 ICT elements from the perspective of an administrator or network operator with privileged access. The ICT element criticality assessments can be analyzed collectively to prioritize supply chain risk management efforts.

DHS conducted and continues to refine its assessments[vii] of element criticality and risk. This analysis contains sensitive information and is not included in this public document.

IMPLICATIONS FOR THE FIFTH GENERATION (5G) NETWORK

5G, the next generation mobile network, represents a complete transformation of telecommunication networks. Combining new and legacy elements and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology. As 5G technologies are deployed, some elements may become more or less critical due to increasing or decreasing reliance upon them, or changes in how they are used. Distributed antenna systems will continue to be used in 5G, but the use of small cells[viii] and differing spectrum bands may change how a DAS is utilized. eNodeB/5G NR are 5G fixed communications locations that relay information to and from a transmitting or receiving unit, such as a mobile phone. eNodeB/5G performs a similar function as eNodeB (4G LTE) and NodeB (4G) elements, and as we move towards 5G, the criticality of elements from previous generations may require reassessment. GMLC are expected to go away completely once there is a full conversion to 5G networks. It is likely that 5G's development and deployment and other changes to the IT and Communications sectors will require the revaluation of some elements' criticality, and potentially the introduction of new elements to this assessment.

FUTURE ANALYSIS

DHS' initial analysis in response to Executive Order 13873 is foundational and will support future ICT supply chain analysis. Topics for future analysis may include:

- **Identify and Assess the Criticality of Elements in Other Sectors:** DHS will work with SMEs from other sectors and expand upon this analysis to identify and assess the ICT elements critical to those sectors.
- **Identify and Assess Specific Makes, Models, and Versions of Hardware, Software, and Services:** DHS' initial assessment and methodology may be used in follow-on analysis to identify elements of ICT hardware, software, and services, including analyzing specific products and services to understand the potential vulnerabilities they introduce and the potential consequences they pose.
- **Identify and Evaluate Entities that Manufacture or Provide Critical ICT Elements:** DHS may identify the key suppliers and manufacturers of critical ICT elements, and work with the Office of the Director of

not support military operations. Future analysis is planned to identify specific elements whose compromise would have potentially more significant consequences based on system deployment use cases.

[vi] Manageably Critical elements are still critical. There could still be significant national security consequences if key mitigations are not in place—such as vendor diversity, element redundancy, and encryption.

[vii] The list of ICT element criticality assessments, while "final," is not a permanent list, but will be dynamic and updated periodically to reflect current data on supply, demand, concentration of production, innovation in ICT sectors, new vulnerability considerations, and new mitigation considerations. This final list will serve as the Department of Commerce's initial focus as it develops its report to comply with Executive Order 13873.

[viii] Small cells and micro cells are miniature cellular towers that transmit short-range radio signals.

National Intelligence (ODNI) to incorporate threat analysis into its ICT supply chain analyses. Additionally, DHS reviewed the ODNI EO 13873 response before finalizing this report and found that the two products are complementary for meaningful subsequent analysis.

- **Identify the Most Critical Users of Critical ICT Elements:** DHS may identify entities within the United States whose use of compromised ICT Elements could result in the greatest consequences.
- **Identify or Assess Technology Serving Primarily Physical Purposes:** DHS may expand its list of elements to include Operations Technology (OT), such as programmable logical controllers (PLCs), and Internet of Things (IoT) technology, such as networked thermostats and telematics equipment, which serve primarily physical purposes.[ix]
- **Compare the Consequences of Data Theft with the Consequences of System Damage or Disruption:** It is likely that the set of entities identified as having high potential consequences from data theft will be different from the set of entities identified as having high potential consequences from damage or disruption.
- **Evaluate the Potential Impacts from Mitigation Activities:** DHS may evaluate the potential impacts to U.S. entities from various mitigation activities. This could include evaluating how identified threats might respond to mitigation actions taken by U.S. entities, including the Federal Government, and what the possible consequences of those responses would be for national security. DHS' written assessment may be used in follow-on analysis to analyze potential threat countermoves and their possible consequences.
- **Analyze ICT Elements Throughout the ICT Supply Chain Phases:** DHS may evaluate elements and assess risk throughout each phase of the supply chain:[2]
  - Phase 1: Design
  - Phase 2: Development and Production
  - Phase 3: Distribution
  - Phase 4: Acquisition and Deployment
  - Phase 5: Maintenance
  - Phase 6: Disposal

[ix] DHS defines IoT as "the connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems."

APPENDIX A: NATIONAL CRITICAL FUNCTIONS

NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. This assessment focuses on the *Connect* theme of the National Critical Functions list as it covers the backbone of national connectivity that enables cross-country and global operations. Please see table 2 below:

TABLE 2—NATIONAL CRITICAL FUNCTIONS

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health	▪ Exploration and Extraction of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

DHS' assessment specifically addresses the following National Critical Functions (NCFs) within the *Connect* theme:

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. The focus on NCFs within these sectors was due to the extensive dependence of these NCFs on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences.

APPENDIX B: GLOSSARY

Broadcast Networks: Identified as a sub-role in the ICT Framework. Networks consisting of free and subscription-based, over-the-air radio and television (TV) stations that offer analog and digital audio and video programming services and data services.

Cable Access Points: Identified as a sub-role in the ICT Framework. Systems offering access to analog and digital video programming services, digital telephone service, and high-speed broadband services. Utilizes a mixture of fiber and coaxial cable commonly referred to as a hybrid fiber/coaxial (HFC) network to provide bi-directional signal paths to the customer.

***Connect* Theme (of National Critical Functions):** The NCF *Connect* theme contains nine critical functions, including: Operate Core Network; Provide Cable Access Network Services; Provide Internet Routing, Access, and Connection Services; Provide Radio Broadcast Access Network Services; Provide Position, Navigation, and Timing Services; Provide Internet-Based Content, Information, and Communication Services; Provide Satellite Access Network Services; Provide Wireless Access Network Services; and Provide Wireline Access Network Services.

Core Networking Systems: Identified as a sub-role in the ICT Framework. Core networking systems (also known as “backbone” systems when used to describe internet networks) facilitate the exchange of information among various sub-networks.

Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

Criticality Criteria: Criticality criteria considers important factors that will have the greatest impact on consequences.

End User Equipment and Edge Networking Equipment: Identified as a sub-role in the ICT Framework. End user equipment is any device used by an end-user to communicate, while edge networking equipment provide an entry point for end user equipment to connect into core networking systems. Examples include cellular phones, desktop and laptop computers, and tablets; related local area network infrastructure; and related software.

ICT Element: An ICT element is a type of hardware, software, or service.

ICT Element Core Factors: Core factors are the low-level functional operations performed by individual ICT elements that collectively contribute to determining overall criticality of the element.

ICT Framework: The ICT Framework is comprised of generic representation of ICT systems, which will serve as an organizing principle for binning ICT elements and drawing basic judgements about criticality.

Independent Mitigation: Non-element functions obviate concerns. This is one criticality criterion used by the National Risk Management Center to make criticality determinations.

Local User Access: One of five determined ICT Framework roles. Systems facilitating individual or group user access, via devices, to telecommunications and internet resources.

Long Haul and Short Haul Networks: Identified as a sub-role in the ICT Framework. Communication networks spanning both long and short distances.

Manageably Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.

Mobile Networks: Identified as a sub-role in the ICT Framework. Also known as "cellular networks." A communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver. When joined together, these cells provide radio coverage over a wide geographic area.

National Critical Functions (NCFs): NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof.

Not Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element is unlikely to have significant regional or national impacts.

Processing: One of five determined ICT Framework roles. Systems supporting the creation and manipulation of data or information for a variety of purposes.

Roles: Roles are represented as the five top-level headings of the ICT Element Framework (local user access, transmission, storage, processing, and system management). ICT roles group ICT elements into broad categories of ICT operations they facilitate.

Satellite Access Points: Identified as a sub-role in the ICT Framework. Systems offering access to platforms launched into orbit to relay voice, video, or data signals as part of a telecommunications network.

Security and Operations: Identified as a sub-role in the ICT Framework. Devices, services, and software that provide security and operational functions within a network.

Security Features: Hardware, software, and services that are integrated into ICT systems to provide protection from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide (i.e., anti-virus/anti-malware, IDS/IPS, encryption, authentication, etc.).

Sensitive: An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data's confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

Sub-Roles: Sub-Roles further group ICT elements into narrower operational roles under each of the five ICT roles. ICT elements are decomposed under the sub-roles they support.

Storage: One of five determined ICT Framework roles. Systems supporting retention of data generated by computers and other devices generated either locally or remotely.

Storage and Cloud Based Delivery: Identified as a sub-role in the ICT Framework. Computer data storage and delivery, either on a local server, or (in the case of cloud-based) on multiple servers across multiple locations.

System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[3]

System Management: One of five determined ICT Framework roles. Devices, services, and software serving functions required for system operation, security, and maintenance.

Transmission: One of five determined ICT Framework roles. Systems supporting the process of sending data over a communication medium to one or more computing, network, transit network, communication or electronic devices in a point-to-point, point-to-multipoint, or multipoint-to-multipoint environment.

Wireless Local Area Networks: Identified as a sub-role in the ICT Framework. Systems offering access to telecommunication in which electromagnetic waves (rather than wire) carry the signal over part of or the entire communication path.[x]

Wireline Access Points: Identified as a sub-role in the ICT Framework. Circuit- and packet-switched networks via copper, fiber, and coaxial transport media.

[x] Wireless technologies consist of cellular phones, wireless hot spots (WiFi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services to provide communication services.

[1] President of the United States. Executive Order 13873—Securing the Information and Communications Technology and Services Supply Chain. May 15, 2019. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain. Accessed on January 16, 2020.

[2] DHS/CISA/NRMC. December 2018. Supply Chain Risks for Information and Communication Technology. https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_nrmc_supply-chain-risks-for-information-and-communication-technology.pdf. Accessed on January 16, 2020.

[3] NIST. Computer Security Resource Center. "System." 2019. https://csrc.nist.gov/glossary/term/system. Accessed on January 16, 2020.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@cisa.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management.

PDM19058