Cybersecurity and Infrastructure Security Agency

March 13, 2020; 1500 EDT

FREQUENTLY ASKED QUESTIONS (FAQs): DHS's ICT METHODOLOGY IN SUPPORT OF EXECUTIVE ORDER 13873

What is the purpose of the report? What is its intended use?

In response to Executive Order (EO) 13873, DHS developed a methodology for assessing Information and Communication Technology (ICT) elements (hardware, software, and services) to determine which elements present vulnerabilities that pose the greatest consequences to U.S. critical infrastructure, National Critical Functions,[i] and national security. The U.S. Department Homeland Security (DHS) used this methodology to produce sensitive criticality assessments for each element consistent with requirements of EO 13873. This methodology should not be interpreted as a comprehensive risk methodology.

Are "criticality" and "consequence" the same thing?

Not exactly, but national security consequences are a primary factor in determining criticality for the purposes of this methodology. Criticality is a culmination of several factors. The first step in determining criticality of an ICT element requires identifying how important an element is to the operations of the function (e.g., wireless local area networks) it supports. The next step involves identifying the importance of confidentiality, integrity, and availability of the information flowing over the element; the importance of the function it supports; and what damage it could cause to national security if compromised. Elements of similar criticality may be more or less consequential depending on the users of that element. For example, an element relied upon by the U.S. military may be more consequential than a similar element used by a local grocery store. Compromise of both elements could affect operations or data security, but one would have much more significant consequences and therefore warrant much more significant scrutiny.

Why doesn't DHS's methodology factor in threat analysis?

DHS did not incorporate threat information into the ICT supply chain methodology because the EO tasked the Office of the Director of National Intelligence (ODNI) to conduct threat analysis in support of the overall effort. As such, DHS's analysis is only designed to address certain vulnerability and consequence analysis as portions of the overall risk equation.

How can the ICT methodology be used to assess ICT risk?

DHS's assessment can be used as an input to a risk assessment, but by itself is not sufficient for a comprehensive review of risk. ODNI's threat analysis and additional analysis of economic and public health and safety consequences are required to conduct a more comprehensive assessment of risk. For example, if 10 different U.S. entities use an element, and there are 10 different suppliers, there are potentially 100 different risks. If only one of the 10 entities would have high consequences from compromise, and only one of the 10 suppliers are considered high threat, then there is only 1 scenario out of 100 that would be both high threat and high consequence. Depending on risk tolerance, this may be the only scenario that requires

[i] 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.

mitigation, while all other 99 scenarios are considered acceptable. This is a simple example that illustrates why DHS's initial criticality analysis is helpful in providing decision support and identifying areas of interest, but additional inputs are required for a comprehensive risk assessment.

What does "Manageably Critical" mean? Should I be less concerned about "Manageably Critical" elements?

An element designated "Manageably Critical" is still critical, but it has been determined that reliable and reasonable measures mitigate the likely impacts from compromise (on a case-by-case basis). Factors such as a lack of vendor diversity or access to sensitive data could reasonably cause a "Manageably Critical" element to warrant more scrutiny than an element with a "Critical" designation.

Furthermore, it is impossible to fully eliminate risk. Most, if not all, elements within the ICT supply chain have vulnerabilities that adversaries could potentially exploit. The criticality designations are not intended to imply an element is more or less vulnerable to supply chain compromise. They only determine if compromise of such vulnerabilities could reasonably result in a national security impact.

How is DHS's ICT methodology connected to 5G wireless technologies?

While some of the elements analyzed using DHS's methodology are easily connected to 5G network architecture, the deconstruction of the ICT supply chain into 61 elements was intended to encompass as much of the IT and Communications sectors as possible, not just 5G. Future versions of analysis may include new elements that more directly relate to 5G network architecture.

What is "systems software (sensitive)?"

For the purposes of meeting the objectives of the EO, DHS grouped software into two categories: systems software and application software. Systems software includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, software-defined networking, and file management utilities. Application software 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. Systems software compromise would likely have more significant consequences than applications system software due to the increased system privileges inherent within the software.

DHS further divided software based on the type of system it is installed on: sensitive systems and non-sensitive systems. DHS did this because it did not want to treat software installed on national security or critical infrastructure systems (which could have national security impacts) the same as software installed on personal computers or business systems (which does not typically have national security impacts). DHS generally viewed localized instances of data exfiltration from non-sensitive systems as unlikely to rise to the level of a national security concern. DHS recognizes that this is an imperfect calculation, and that a more robust interagency process would be required to determine a more definitive conclusion.

The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the 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 security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.cisa.gov/national-risk-management.

PDM20011