EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

November 1, 2021 - Volume 13, Issue 20

Request for Comments Concerning the Imposition of Export Controls on Certain Brain-Computer Interface (BCI) Emerging Technology

10/26/2021
86 FR 59070

This advance notice of proposed rulemaking (ANPRM) requests feedback from the public and U.S. industry concerning the potential uses of Brain-Computer Interface (BCI) technology, particularly with respect to its impact on U.S. national security (e.g., whether such technology could provide the United States, or any of its adversaries, with a qualitative military or intelligence advantage), and also whether effective export controls could be implemented on such technology. BCI technology has been identified as a technology for evaluation as a potential emerging technology, consistent with the interagency process described in Section 1758 of the Export Control Reform Act of 2018 (ECRA). BCIs provide a direct communication pathway between an enhanced or wired brain and an external device, with bidirectional information flow. BCIs frequently involve a process in which brain signals are acquired, analyzed and then translated into commands that are: (1) used to control machines; (2) potentially transferred to other humans; or (3) used for human assessment or enhancement.

Continued…..

DEPARTMENT OF COMMERCE Bureau of Industry and Security
15 CFR Part 774 [Docket No. 211019–0212] RIN 0694–AI41
Request for Comments Concerning the Imposition of Export Controls on Certain Brain-Computer Interface (BCI) Emerging Technology

*(*Continued On The Following Page)*

NEWSLETTER NOTES

* Request for Comments Concerning the Imposition of Export Controls on Certain Brain-Computer Interface (BCI) Emerging Technology

* EPA unveils strategy to regulate toxic 'forever chemicals'

* Forever Chemical Crackdown could affect CT

* Chicago Tech Executive Guilty of Illegally Exporting Computer Equipment to Pakistan

* CISA's Zero Trust Maturity Model Seeks to Optimize Federal Cybersecurity

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Advance notice of proposed rulemaking (ANPRM).

SUMMARY: The Bureau of Industry and Security (BIS) maintains controls on the export, reexport and transfer (incountry) of dual-use items and less sensitive military items pursuant to the Export Administration Regulations, including the Commerce Control List (CCL). Certain items that could be of
potential concern for export control purposes are not yet listed on the CCL or controlled multilaterally, because they are emerging technologies. Among these items is Brain-Computer Interface (BCI) technology, which includes, interalia, neural-controlled interfaces, mindmachine interfaces, direct neural interfaces, and brain-machine interfaces. BIS is seeking public comments on the potential uses of this technology, particularly with respect to its impact on U.S. national security (e.g., whether such technology could provide the United States, or any of its adversaries, with a qualitative military or intelligence advantage). This document also requests public comments on how to ensure that the scope of any controls that may be imposed on this technology would be effective (in terms of protecting U.S. national security interests) and appropriate (with respect to minimizing their potential impact on legitimate commercial or scientific applications).

DATES: Comments must be received by BIS no later than December 10, 2021.

ADDRESSES: You may submit comments, identified by regulations.gov docket number BIS–2021–0032 or by RIN 0694–AI41, through any of the
following:

• Federal eRulemaking Portal: https://www.regulations.gov. You can find this advance notice of proposed rulemaking by searching for its regulations.gov docket number, which is BIS–2021–0032.

• Email: PublicComments@ bis.doc.gov. Include RIN 0694–AI41 in the subject line of the message. All filers using the portal or email should use the name of the person or entity submitting the comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential submission. For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters ''BC.'' Any page containing business confidential information must be clearly marked ''BUSINESS CONFIDENTIAL'' on the top of that page. https://www.regulations.gov.

*(*Continued On The Following Column)*

FOR FURTHER INFORMATION CONTACT: For questions on Brain-Computer Interface technology, contact Dr. Betty Lee, Chemical and Biological Controls Division, Office of Nonproliferation and Treaty Compliance, Bureau of Industry and Security, U.S. Department of Commerce, (202) 482–5817, Email: Betty.Lee@bis.doc.gov. For questions on the submission of comments, contact Willard Fisher, Regulatory Policy Division, Office of Exporter Services, Bureau of Industry and Security, U.S. Department of Commerce, (202) 482–6057, Email: RPD2@bis.doc.gov.

SUPPLEMENTARY INFORMATION: Background
As part of the National Defense Authorization Act (NDAA) for Fiscal Year 2019, Public Law 115–232, Congress enacted the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. 4801–4852. Section 1758 of ECRA (as codified under 50 U.S.C. 4817) authorizes the Bureau of Industry and Security (BIS) to establish appropriate controls on the export, reexport or transfer (in-country) of emerging and foundational technologies. Pursuant to ECRA, on November 19, 2018, BIS published an advance notice of proposed rulemaking (November 19 ANPRM) (83 FR 58201). That ANPRM identified Brain-Computer Interface (BCI) technology as part of a representative list of technology categories concerning which BIS, through an interagency process, sought public comment to determine whether there are specific emerging technologies that are essential to U.S. national security and for which effective controls can be implemented. Comments to the November 19 ANPRM on Brain-Computer Interface Technology In response to its November 19 ANPRM, BIS received approximately 13 comments related to the potential designation of BCI technology as an emerging technology. The substance of these comments is summarized in the following paragraphs. One respondent noted that BCI technology, although still in the early stages of development, is currently available in Wassenaar Arrangement participating countries (including the United States), as well as in other countries. Similarly, another respondent indicated that emerging BCI technology has important applications in human health care and assistive technologies and that, consequently, overly broad export controls on such technology could hinder research in these areas. In addition, a respondent in the aerospace sector stated that overly broad export controls would discourage information sharing and thereby hinder BCI research and development projects in the aerospace industry. This respondent also urged that license exceptions should apply to those situations involving technological collaboration with our allies. Another respondent noted that the imposition of export controls on the representative general categories of technology (including BCI technology) identified in BIS's November 19 ANPRM would impact the fields of automotive development (e.g., autonomous driving and automotive safety), artificial intelligence, advanced materials development, human-machine interfaces and robotics.

(*Continued On The Following Page)

This respondent expressed the concern that the imposition of overly strict export controls on such technology by the United States could drive future research and development programs to other technologically sophisticated countries in Europe, Asia and the Americas that would not impose unilateral export controls on such technology. As examples of the possible adverse effect of export controls on such technology, this respondent cited the impact that the tightening of export controls had on the U.S. commercial satellite sector and on LiDAR controlled under ECCN 6A001 or ECCN 6A008.j.2. One respondent urged that U.S. export controls on BCI technology be addressed through the establishment of harmonized multilateral controls. Otherwise, the imposition of export controls on such technology by the United States could adversely impact future collaboration with our allies (e.g., foreign companies might become reluctant to utilize U.S.-origin BCI products or technology if they were subject to unilateral export controls). This respondent also recommended that the United States view its national security interests more narrowly, observing that the United States likely would lose credibility in multilateral export control forums if it tried to tie its national security and economic security interests too closely together. This respondent also asked whether these controls would be applied, across-the-board, to all countries or if they would vary depending upon the country of destination. In addition, the respondent inquired as to whether the de minimis provisions in the Export Administration Regulations (EAR) would apply, how often the United States would evaluate and update the scope of these emerging technology controls, and what additional measures (i.e., other than obtaining export or reexport licenses) U.S. companies and non-US entities would be expected to take in order to protect such technology. Another respondent also warned about the potential harm to U.S. technological leadership and competitiveness if the United States were to impose broad unilateral controls on emerging technologies (including BCI technologies), instead of working with our allies to develop and implement multilateral controls. This respondent stressed that any export controls that are imposed on emerging technologies must apply only to those emerging technologies that are determined to be essential to U.S. national security (e.g., export controls on such technologies should address specific U.S. national security concerns, rather than trade policy issues). In addition, this respondent urged that emerging technologies should not be controlled unless they are exclusive to the United States and encompass only core technologies. This respondent also recommended that U.S. controls should focus primarily on technology required for ''development,'' rather than technology for ''production'' or ''use.'' This respondent further urged that, to the extent possible, any future EAR controls on emerging technologies should be designed to complement the existing controls on the Commerce Control List and the EAR definitions that apply to similar items, and not be described in vague terms (e.g., as capable for use with one or more specified items).

(*Continued On The Following Column)

One respondent observed that the digital information field of BCI technology is quite mature and that, consequently, digital information technologies should remain unencumbered for the free exchange and cross-pollination of advancements across borders. In a similar vein, another respondent stated that, if export controls on quantum computing and BCI technologies were not properly crafted, these controls could damage U.S. competitiveness and undermine U.S. technological leadership by slowing development, limiting resources, reducing market participation and limiting collaborative opportunities. This respondent emphasized that, in developing and implementing export controls on such technologies, an effective partnership among government, industry and academia would be essential. Process To Identify and Control Emerging Technology Under ECRA, emerging and foundational technologies are those essential to the national security of the United States, but not described in Section 721(a)(6)(A)(i)–(v) of the Defense Production Act of 1950 (50 U.S.C. 4565(a)), as amended. Section 1758(a) of ECRA (50 U.S.C. 4817(a)) outlines an interagency process for identifying emerging and foundational

59072 Federal Register / Vol. 86, No. 204 / Tuesday, October 26, 2021 / Proposed Rules 1 Krucoff, M.O., Rahimpour, S., Slutzky, M.W., Edgerton, V.R., Turner, D.A. (2016), ''Enhancing Nervous System Recovery through Neurobiologics, Neural Interface Training, and Neurorehabilitation,'' Neuroprosthetics, 10 (584). 2 Binnendijk, A., Marler, T., Bartels, E.M. (2019), ''Brain-Computer Interfaces: U.S. Tactical Military Applications and Implications,'' RAND Report RR–2996–CGRS. technologies. This process considers both public and classified information, as well as information from the Emerging Technology Technical Advisory Committee and the Committee on Foreign Investment in the United States. In identifying specific emerging technologies, this process also takes into account all of the following:

- The development of the emerging technologies in foreign countries;
- The effect export controls might have on the development of the emerging technologies in the United States; and
- The effectiveness of export controls on limiting the proliferation of the

emerging technologies in foreign countries.

In addition, Section 1758(a)(2)(C) of ECRA (50 U.S.C. 4817(a)(2)(C)) requires that the interagency process for identifying emerging technologies include a notice and comment period. The Secretary of Commerce must establish appropriate controls on the export, reexport or transfer (in-country) of technology identified pursuant to the Section 1758 process.

(*Continued On The Following Page)

In so doing, the Secretary must consider the potential end-uses and end-users of emerging and foundational technologies, and the countries to which exports from the United States are restricted (e.g., embargoed countries). While the Secretary has discretion to set the level of export controls, at a minimum a license must be required for the export of such technologies to countries subject to a U.S. embargo, including those countries subject to an arms embargo. BCI technology has been identified as a technology for evaluation as a potential emerging technology, consistent with the interagency process described in Section 1758 of ECRA. Consequently, BIS is publishing this ANPRM to obtain feedback from the public and U.S. industry concerning whether such technology could provide the United States, or any of its adversaries, with a qualitative military or intelligence advantage. Fundamentally, BCIs provide a direct communication pathway between an enhanced or wired brain and an external device, with bidirectional information flow.1 BCIs frequently involve a process in which brain signals are acquired, analyzed and then translated into commands that are: (1) Used to control machines; (2) potentially transferred to other humans; or (3) used for human assessment or enhancement. Medical uses of BCI technology include replacing or restoring useful function to people disabled by neuromuscular disorders such as amyotrophic lateral sclerosis, cerebral palsy, stroke, or spinal cord injury. BCI technology can also be a promising interaction tool for the public, with many potential applications in multimedia, entertainment and other fields. This technology will also have potential for military use in enhancing the capabilities of human soldiers, including collaboration for improved decision making, assisted-human operations, and advanced manned and unmanned military operations.2 Although the ability to apply BCI technology remains subject to certain limitations (e.g., approximately 15–30% of individuals currently are thought to be unable to produce brain signals robust enough to operate a BCI), the scientific community is addressing these limitations through strategies such as: (1) An adaptive machine learning approach that incorporates neurophysiological and psychological traits; and (2) the development of more advanced sensors (e.g., a coordinated network of independent, wireless microscale neural sensors that are able to gather data from much larger groups of brain cells than most current BCI systems).

Request for Comments Consistent with Section 1758(a)(2)(C) of ECRA (50 U.S.C. 4817(a)(2)(C)), this ANPRM provides the public with notice and the opportunity to comment for the purpose of evaluating BCI technology as an emerging technology. Consequently, BIS welcomes comments on this ANPRM that would address, but not necessarily be limited to, the following questions. If specific BCI systems are discussed as part of any response to these questions, the public is requested to address the effectiveness of such systems (e.g., with respect to validation, assessment, detection of errors and ability to operate, as intended, for all types of individuals)

*(*Continued On The Following Column)*

(1) What specific uniform standards for BCI technology would need to be adopted to ensure their application on a global basis (i.e., as international standards for BCI technology)?
(2) Where does the development of BCI in the United States stand with respect to other countries (e.g., is the United States on the forefront of BCI technology development)?
(3) Is BCI technology currently available for commercial use in certain foreign countries and, if so, where and for what specific purposes (e.g., have foreign companies already developed devices or chips for specific commercial applications)?
(4) Has the current stage of development with respect to invasive and/or non-invasive BCI technology reached the point at which such technology is ready for commercial production and use?
(5) Is the main progress with respect to non-invasive brain signal sensors being made in terms of real-time algorithms designed to transform neural signals into commands (i.e., what is developing faster: ''software'' (algorithms) or hardware (sensors))?
(6) What impact would the establishment of export controls on BCI technology have on U.S. technological leadership (i.e., not only in the field of BCI technology, but overall) and would this impact be distinctly different if controls were placed primarily on ''software'' as opposed to hardware, or vice versa?
(7) How is the future development of artificial intelligence (AI) technology or other emerging technologies likely to impact the development of BCI technology, or vice versa?
(8) What types of ethical or policy issues are likely to arise from the use of BCI technology (e.g., for medical or military purposes)?
(9) What kinds of risks and benefits currently exist, or are likely to arise, as a result of the application of BCI technology?
(10) What are the potential advantages or disadvantages of using invasive and non-invasive BCI chips/sensors and related ''software'' (e.g., algorithms for signal processing) for specific applications? To what extent would these advantages or disadvantages correspond (or differ) based upon whether invasive or non-invasive BCI chips/sensors and related ''software'' were being used?
(11) Are there any BCI technologies that are significantly more vulnerable than others to cybersecurity threats (e.g., military systems employing BCI technologies that could adversely impact U.S. biodefense)?
(12) What is the potential for transmitted BCI data to be hacked or manipulated to influence the user or machine? Is such data inherently more vulnerable to hacking or manipulation than other forms of data? Would the invasive or non-invasive characteristics of BCI data have any impact on the potential vulnerability of such data?

(*Continued On The Following Page)

Federal Register /Vol. 86, No. 204 /Tuesday, October 26, 2021 / Proposed Rules 59073 In addition to public comments that would assist BIS in evaluating the status of BCI technology as an emerging technology, BIS encourages comments that would help it to determine: (1) Which aspects of BCI technology would be more likely to require monitoring by the U.S. Government (USG); and (2) Whether specific USG policies and regulations, as well as industry standards, need to be established before this technology becomes widely available for use in commercial applications. BIS also welcomes comments concerning whether export controls on BCI technology should be implemented multilaterally (rather than unilaterally), in the interest of increasing their effectiveness and minimizing their impact on U.S. industry. As noted above, a number of respondents who commented on BIS's November 19 ANPRM indicated their preference for multilateral export controls over unilateral export controls, because the former typically place U.S. industry on a more level playing field versus producers/suppliers in other countries. In this regard, note that Section 1758(c) of ECRA (as codified under 50 U.S.C. 4817(c)) provides that ''the Secretary of State, in consultation with the Secretary [of Commerce] and the Secretary of Defense, and the heads of other Federal agencies, as appropriate, shall propose that any technology identified pursuant to subsection (a) [of ECRA] be added to the list of technologies controlled by the relevant multilateral export control regimes.'' Subsection (a) of section 1758 (as codified under 50 U.S.C. 4817(a)) addresses the interagency process for identifying emerging technologies. BIS also encourages comments that address issues raised in the November 19 emerging technology ANPRM public comments (as summarized above) and any other BCI technology topics that they consider to be relevant to this inquiry. The information provided by the respondents in response to this ANPRM will assist BIS in evaluating BCI as a potential emerging technology for the purpose of formulating export control policies that will be both effective and appropriate, with respect to their objective and scope. Comments should be submitted to BIS as described in the ADDRESSES section of this ANPRM and must be received by BIS no later than December 10, 2021. This rule has been designated a ''significant regulatory action,'' although not economically significant, under Executive Order 12866. Accordingly, this rule has been reviewed by the Office of Management and Budget (OMB).

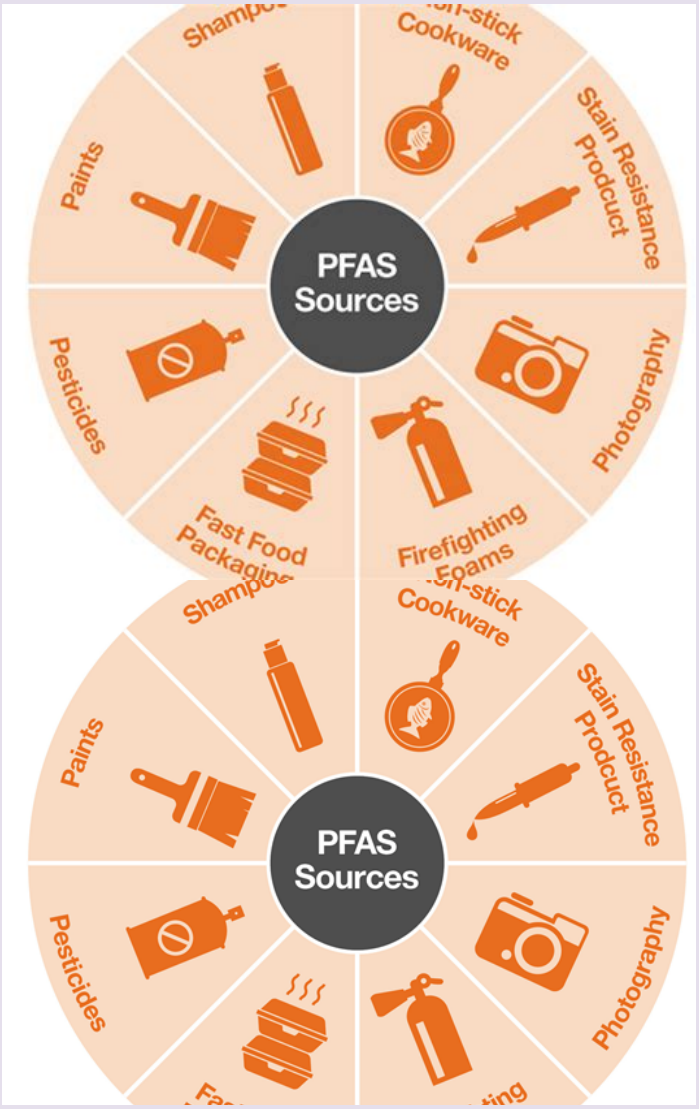
Matthew S. Borman,
Deputy Assistant Secretary for Export Administration.

Forever Chemical Crackdown could affect CT

NEW HAVEN, Conn. (AP) — The Biden administration's proposed crackdown on so-called "forever chemicals" used in products from makeup to cookware could have a wide-ranging impact on Connecticut manufacturers.

Last week's EPA announcement covers per- and polyfluorinated alkyl, substances known as PFAS that are considered long-term health threats in food and water supplies.

https://www.argus-press.com/news/national/article_37dbcc9b-498e-55da-b459-8ee6f1075100.html



Chicago Tech Executive Guilty of Illegally Exporting Computer Equipment to Pakistan

CHICAGO —A Chicago technology executive pleaded guilty today to a federal criminal charge and admitted illegally exporting computer equipment from the United States to a nuclear research agency of the Pakistani government.

OBAIDULLAH SYED, 66, of Northbrook, Ill., pleaded guilty to conspiracy to export goods from the U.S. without a license from the Department of Commerce and to submit false export information. The conviction is punishable by a maximum sentence of five years in federal prison and a maximum fine of $250,000. U.S. District Judge Mary M. Rowland set sentencing for Feb. 23, 2021, at 12:30 p.m. The guilty plea was announced by John R. Lausch, Jr., United States Attorney for the Northern District of Illinois; Angie Salazar, Special Agent-in-Charge of the Chicago office of Homeland Security Investigations; Aaron Tambrini, Special Agent-in-Charge of the U.S. Department of Commerce, Bureau of Industry and Security-Office of Export Enforcement, Chicago Field Office; and Cynthia A. Bruce, Special Agent-in-Charge of the U.S. Department of Defense, Defense Criminal Investigative Service, Southeast Field Office. The government is represented by Assistant U.S. Attorney Peter M. Flanagan.

Syed owned Pakistan-based BUSINESS SYSTEM INTERNATIONAL PVT. LTD., and Chicago-based BSI USA. The companies provided high-performance computing platforms, servers, and software application solutions. Syed admitted in a plea agreement that from 2006 to 2015 he conspired with his company's employees in Pakistan to violate the International Emergency Economic Powers Act by exporting computer equipment from the U.S. to the Pakistan Atomic Energy Commission without obtaining the required authorization from the U.S. Department of Commerce. The PAEC is a Pakistani government agency responsible for, among other things, designing and testing explosives and nuclear weapons parts. It was designated by the U.S. government as an entity which may pose an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States. Syed further admitted that he and the other conspirators falsely represented to U.S.-based computer manufacturers that the illegal shipments were intended for Pakistan-based universities or Syed's businesses, when, in fact, the conspirators knew that the true end user of each shipment was either the PAEC or a research institute that trained the agency's engineers and scientists. In so doing, Syed and his company caused the U.S.-based computer manufacturers to submit to the U.S. government shipping documents that listed false end-users for the U.S.-origin goods, thereby undermining the U.S. government's ability to stop the illegal shipments.

Business System International Pvt. Ltd. was charged in the conspiracy as a corporate defendant. The company has yet to respond to the charges.

CISA's Zero Trust Maturity Model Seeks to Optimize Federal Cybersecurity

Published: September 23, 2021

The path to zero trust for federal agencies will be an incremental journey that will take years to implement.

The Cybersecurity and Infrastructure Security Agency (CISA) recently released a draft Zero Trust Maturity Model (ZTMM) for public comment, providing federal agencies with "a road map to migrate and deploy zero trust security concepts to an enterprise environment."

In the introduction, CISA says the pre-decisional draft document is "designed to be a stopgap solution to support Federal Civilian Executive Branch (FCEB) agencies in designing their zero trust architecture (ZTA) implementation plans" in line with the White House's May Executive Order (EO) on improving federal cybersecurity.

Three Stages of Zero Trust Maturity

CISA identifies three stages agencies will migrate through on their way to Zero Trust maturity, each with increasing levels of protection, detail, and complexity for adoption. The Traditional stage is characterized by manual, inflexible or proprietary security processes and policy enforcement. The Advanced stage includes some cross-pillar coordination and inputs/outputs with centralized visibility, control, and policy enforcement with some least-privilege access controls. The Optimal stage involves fully automated security attribute processes, dynamic policy enforcement, open standards for interoperability, and centralized visibility with historian functionality.

Zero Trust Maturity Across Five Technology Pillars

The CISA ZTMM presents a gradient of implementation across five distinct technology pillars – Identity, Device, Network, Application Workload, and Data – where incremental advancements can be made over time toward optimization. Each pillar also includes areas of opportunity for maturity around Visibility and Analytics, Automation and Orchestration, and Governance.

Pillar #1 Identity – An identity refers to an attribute or set of attributes that uniquely describe an agency user or entity. Identity functions pertaining to zero trust include:

*(*Continued On The Following Page)*

- Authentication – Agency moves from authenticating identity using either passwords or multi-factor authentication (MFA) to optimize by continuously validating identity, not just when access is initially granted.
- Identity Stores – Agency matures from only using on-premises identity providers to federating some identity with cloud and on-premises systems and eventually optimizing with global identity awareness across cloud and on-premises environments.
- Risk Assessment – Agency moves from making limited determinations for identity risk and determining risk based on simple analytics and static rules to optimizing risk determination and protections by analyzing user behavior in real time with machine learning algorithms.

  Cloud Implications – As agencies migrate services to the cloud, their users will have identities among a variety of providers, so agencies will need to integrate their on-premises identities with those in the cloud environments to effectively manage and secure these identities.

Pillar #2 Device – A device refers to any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, and others. Device functions pertaining to zero trust include:

- Compliance Monitoring – Agency matures from having limited visibility into device compliance to employing compliance enforcement mechanisms for most devices, eventually optimizing by constantly monitoring and validating device security posture.
- Data Access – Agency moves from allowing access to data without visibility into the accessing device to evaluating device posture on first-access, optimizing to managing data access with real-time risk analytics about devices.
- Asset Management – Agency evolves from manual device inventory tracking to automated device management and patching, optimizing by integrating asset and vulnerability management across all environments, including cloud and remote.

Pillar #3 Network/Environment – CISA refers to a network as any open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages. Network functions pertaining to zero trust include:

*(*Continued On The Following Column)*

- Network Segmentation – Agency moves from defining their network architecture using large perimeter/macro-segmentation to defining more of their network architecture by ingress/egress micro-perimeters with some internal micro-segmentation, eventually optimizing on a network architecture consisting of fully distributed ingress/egress micro-perimeters and deeper internal micro-segmentation based around application workflows.
- Threat Protection – Agency evolves from threat protections based primarily on known threats and static traffic filtering and basic analytics to proactively discover threats to optimization through integrating machine learning-based threat protection and filtering with context-based signals.
- Encryption – Agency matures from encrypting minimal internal or external traffic to encrypting all traffic to internal applications, optimizing by encrypting all traffic to internal and external locations, where possible.

Pillar #4 Application Workload – Applications and workloads include agency systems, computer programs and services that execute both on-premise and in a cloud environment. Application Workload functions pertaining to zero trust include:

- Access Authorization – Agency access to applications evolves from local authorization and static attributes to centralized authentication, authorization, monitoring, and attributes, eventually optimizing to continuous authorization for applications access, considering real-time risk analytics.
- Threat Protections – Agency threat protections mature from minimal integration with application workflows with general purpose protections to incorporate basic integration of threat protections with application-specific protections, optimizing on strongly integrated threat protections with analytics to provide protections based on application behavior.
- Accessibility – Agency advances from some critical cloud applications being directly accessible to users over the internet, with all others available through a virtual private network (VPN) to eventually optimize by making all applications directly accessible to users over the internet and eliminating the need for VPNs.
- Application Security – Agency evolves from performing application security testing prior to deployment to integrating application security testing into the application development and deployment process, eventually optimizing by integrating regular automated testing of deployed applications.

(*Continued On The Following Page)

Pillar #5 Data – Agency data should be protected on devices, in applications, and on networks, while at rest and in transit. Data functions pertaining to zero trust include:

- Inventory Management – Agency evolves from manual processes to categorize and inventory data to increasingly use automation for data categorization and tracking, eventually optimizing by continuously inventorying data with robust tagging and tracking and augmenting categorization with machine learning models.
- Access Determination – Agency matures from governing data access through static access controls to using least privilege controls that consider identity and risk, optimizing to dynamic, risk-based data access with just-in-time and just-enough principles.
- Encryption – Agency matures from primarily storing data unencrypted in on-premises data stores to storing data encrypted in cloud or remote environments, optimizing to encrypting all data at rest.

The CISA model was released in coordination with the White House release of its draft Zero Trust Strategy to improve cybersecurity government-wide.

CISA and others recognize that the path to zero trust will be an incremental journey that will take years to implement. One particular challenge is dealing with and modernizing legacy IT infrastructure and systems that may not readily support a zero trust implementation.

CISA is seeking industry comments on some key questions around their draft ZTMM through Friday, October 1, 2021.

"The best preparation for good work tomorrow is to do good work today."

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

EIB World Trade Headlines
Evolutions In Business • www.eib.com • (978) 256-0438 • P.O. Box 4008, Chelmsford, MA 01824