INSTITUTE FOR DEFENSE ANALYSES

Overview of Laws Governing the Potential Tracking of Students across DoD-Funded Science, Technology, Engineering, and Mathematics (STEM) Outreach Programs

Stephen M. Olechnowicz, Project Leader

Michael S. Nash

W. Thomas Strickland

Ransee Peshala Wimalasena

June 2021

Approved for public release;
distribution is unlimited.

IDA Document D-21630

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project BC-5-330912, "DoD Cyberspace Workforce Professionalization," for the Cyber Workforce Management Director, DoD Chief Information Officer. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Elizabeth McDaniel, James M. Jenkins, Tara C. McFeely

For More Information

Stephen M. Olechnowicz, Project Leader
solechno@ida.org, 703-845-6633

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-21630

Overview of Laws Governing the Potential Tracking of Students across DoD-Funded Science, Technology, Engineering, and Mathematics (STEM) Outreach Programs

Stephen M. Olechnowicz, Project Leader
Michael S. Nash
W. Thomas Strickland
Ransee Peshala Wimalasena

Executive Summary

The Cyber Workforce Management Directorate in the office of the Department of Defense (DoD) Chief Information Officer (CIO) tasked the Institute for Defense Analyses (IDA) with researching the legality of tracking K-12 students who participate in DoD-sponsored science, technology, engineering, and mathematics (STEM) outreach programs. This issue arose out of a congressional request for recommendations in the National Defense Authorization Act for Fiscal Year 2021 (NDAA FY 2021) Section 1726 titled, "Department of Defense Cyber Workforce Efforts."[1]

Section 1726 subsection (c), "Alignment of Cybersecurity Training Programs," directs the Secretary of Defense to submit to the congressional defense committees a report on how to better align and harmonize the Department of Defense (DoD) programs, initiatives, and investments to train elementary, secondary, and postsecondary students in fields related to cybersecurity, cyber defense, and cyber operations, as described in the NDAA FY 2020 Section 1649.[2]. Part (2) under subsection (c) specifically outlines that the report must also provide recommendations for mechanisms to track participation and transition of participation from one such program to another.[3] The full text of Section 1726 and Section 1649 appear in Appendix A and Appendix B, respectively.

On January 13, 2021, the IDA team, DoD CIO sponsor, and executive leaders from the office of the Under Secretary of Defense for Research and Engineering (USD(R&E)), the office of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), and the National Security Agency (NSA) met with the House Armed Services Committee (HASC) staff member who authored Section 1726. The staff member's feedback indicates that Congress seeks to assess the success of DoD's STEM outreach programs in strengthening its leverage in the recruitment of civilian and military cyber workforces by raising student awareness of cyber careers and encouraging students to obtain suitable education and training in pursuit of such careers within DoD or other Federal agencies. DoD focuses on STEM education outreach because it recognizes that STEM provides the multidisciplinary foundation for cyber education and training.

---

[1] Pub. L. 116-283, *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, January 1, 2021, 1875.

[2] Pub. L. 116-92, *National Defense Authorization Act for Fiscal Year 2020*, 133 Stat. 1758, December 20, 2019.

[3] [Paragraph (c)(2)(C) of Section 1726 of the NDAA FY 2021].

Such tracking mechanisms necessitate DoD to track student participation across its STEM outreach programs, as well as any student participant's subsequent entry into DoD employment.

If DoD were to recommend such a tracking capability to Congress, DoD STEM program offices must fully understand privacy issues related to the rights of students, especially minors, and Personally Identifiable Information (PII) under the Privacy Act of 1974 and other Federal laws. The IDA team conducted a literature review and interviewed a DoD privacy expert to produce this document, which provides an overview of the initial research on Federal laws and applicable DoD issuances regarding the privacy rights of minors, the handling of PII, and the potential legal ramifications of establishing a DoD-wide tracking system for student participation in its STEM outreach programs.

Given that many DoD-supported STEM education outreach programs focus on elementary and secondary level students who are minors, the IDA team researched the Children's Online Privacy Protection Act (COPPA, 1998), the Protection of Pupil Rights Amendment (PPRA, 1978), and the Family Educational Rights and Privacy Act (FERPA, 1974) to understand the rights afforded by those laws to minors. FERPA applies to Department of Education (DoEd)-funded educational institutions, and it permits, under certain conditions, the disclosure of student PII from education records. Therefore, in the case of DoD STEM outreach programs that partner with DoEd-funded educational institutions, the burden is on such institutions to determine the exceptions under which disclosure of PII without consent is permitted or to obtain consent if deemed necessary.

The IDA team also interviewed a Senior Privacy Management Analyst in DoD's Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) regarding DoD Instruction 5400.11, *DoD Privacy and Civil Liberties Programs* (2019), and DoD 5400.11-R, *Department of Defense Privacy Program* (2007). DoD 5400.11-R provides guidance on the Privacy Act of 1974, which is essential to understanding the lawful handling of PII, and provides direction on the procedures that DoD must follow to collect, store, and retrieve any PII that will be part of a potential tracking mechanism, regardless of the age of the participant to whom the record pertains.

Table EX-1 summarizes all privacy-related laws relevant to this research.

Table EX-1. Summary of Pertinent Federal Laws

COPPA	• Issues and enforces regulations concerning the online privacy of minors by giving parents control over the information that websites can collect from minors. • Protects minors under 13 years of age. • Applies to operators of commercial and general audience websites and online services, which includes mobile apps and smart devices.

	• Applies to web-based services used by schools such as homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. • Allows schools to consent to the collection of information on the parents' behalf as long as it is limited to the educational context. • Prohibits operators from conditioning a minor's participation in an online activity on the minor providing more information than is reasonably necessary to participate in that activity.
PPRA	• Affords parents the right to consent before their children participate in certain surveys, certain physical exams, and the collection of information used for marketing purposes. • Applies to a survey if it concerns one or more of eight protected information areas (protected information survey).
FERPA	• Prohibits the disclosure of PII in student education records to third parties without parental consent. • Applies to all educational institutions that receive funding from the DoEd. • Schools may disclose "directory information" (which includes information (students' names, addresses, and telephone listings) without consent. • Includes exceptions that permit data sharing under certain conditions with agencies, vendors, or individuals to conduct studies, audit or evaluate programs, and enforce or comply with related Federal legal requirements. • DoEd provides a "cheat sheet" for schools to understand the most commonly used exceptions to the FERPA written consent requirement. • Burden of obtaining consent is on the educational institutions receiving DoEd funding.
Privacy Act	• Regulates the collection, maintenance, use, and dissemination of PII by Federal executive branch agencies. • Makes no age delineations regarding the handling of PII. • Requires Federal agencies to publish a SORN in the Federal Register prior to storing and retrieving PII from a SOR. • Permits the collection and retrieval of PII, as long as a PAS is provided to the individual, or a parent in the case of minors, at the point of collection. • A PAS states how non-disclosure of information may impact the benefits the individual may receive from the activity in which they are participating.

NDAA FY 2021 Section 1726(c)(2)(C) requires DoD to recommend mechanisms to track student participation across its cyber-related education outreach programs; however, these programs include students who are minors, and tracking minors is a complicated legal issue due to concerns about minors' privacy rights. Before tracking minor students, DoD must assure that it is lawful to use their PII to track them for the purposes described by Congress; if lawful, DoD should determine how to do this while complying with all privacy-related laws.

The IDA team did not delve into the resource requirements or processes involved in developing a system for tracking participation. Further research is needed to recommend specific tracking mechanisms if DoD chooses to implement such a capability.

Contents

Figures and Tables

1. Introduction

The Cyber Workforce Management Directorate in the office of the Department of Defense (DoD) Chief Information Officer (CIO) tasked the Institute for Defense Analyses (IDA) with researching whether applicable laws permit tracking participation of K-12 students in DoD-sponsored science, technology, engineering, and mathematics (STEM) outreach programs. This issue arose out of a congressional request for recommendations in Section 1726 of the National Defense Authorization Act for Fiscal Year 2021 (NDAA FY 2021).[4]

Section 1726 details requirements regarding the Department of Defense (DoD) cyber workforce efforts. Specifically, subsection (c), "Alignment of Cybersecurity Training Programs," directs the Secretary of Defense to submit to the congressional defense committees a report "containing recommendations on how cybersecurity training programs described in Section 1649 of the National Defense Authorization Act for Fiscal Year 2020 can be better aligned and harmonized."[5] Section 1649 refers to DoD's "efforts, programs, initiatives, and investments to train elementary, secondary, and postsecondary students in fields related to cybersecurity, cyber defense, and cyber operations."[6]

Paragraph (c)(3) of Section 1726, "Cyber Workforce Pipeline and Early Childhood Education," directs the Secretary of Defense to "take into consideration existing Federal childhood cyber education programs," including the programs identified in the report required by Section 1649, as well as the Department of Homeland Security's Cybersecurity Education and Training Assistance Program (CETAP), when completing the report. Furthermore, paragraph (c)(2) of Section 1726 specifically requires that the report provide recommendations concerning "[m]echanisms for tracking participation and transition of participation from one such program to another."[7]

On January 13, 2021, the IDA team, the DoD CIO sponsor, and executive leaders from the office of the Under Secretary of Defense for Research and Engineering (USD(R&E)), the office of the Under Secretary of Defense for Personnel and Readiness

---

[4] Pub. L. 116-283, *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, January 1, 2021, p. 1875.

[5] Pub. L. 116-283.

[6] Pub. L. 116-92, *National Defense Authorization Act for Fiscal Year 2020*, 133 Stat. 1758, December 20, 2019.

[7] Subparagraph (c)(2)(C) of Section 1726 of FY 2021 NDAA, p. 1876]

(USD(P&R)), and the National Security Agency (NSA) met with the House Armed Services Committee (HASC) staff member who authored Section 1726. The staff member's feedback indicates that Congress seeks to assess the outcomes and success of DoD's STEM outreach programs in strengthening its leverage in the recruitment and retention of civilian and military cyber workforces by raising student awareness of cyber careers and encouraging students to obtain suitable education and training in pursuit of such careers within DoD or other Federal agencies. DoD focuses on STEM education outreach because it recognizes that STEM provides the multidisciplinary foundation for cyber education and training.

Tracking mechanisms, as suggested by Section 1726, would necessitate DoD to track the participation of students across its STEM outreach programs, as well as any student participant's subsequent entry into employment in DoD. If DoD were to recommend such a tracking system to Congress, DoD STEM program offices must comply with relevant laws regarding two issues: protecting the privacy rights of minors and lawfully handling Personally Identifiable Information (PII).

1. Protection of the privacy rights of students who are minors.

   Many of DoD's STEM outreach programs focus on elementary and secondary students. Tracking students who are minors raises concerns about minors' privacy rights, DoD must determine whether it can lawfully track minors for the purposes described by Congress and then, if such tracking is determined to be allowed by law, understand how to comply with all laws governing the Federal Government's ability to record and track minors.

2. The collection, maintenance, use, and dissemination of PII.

   Regardless of the age of the participants, if DoD were to collect, maintain, use, or disseminate a participant's PII for the purposes described by Congress, it must comply with general privacy laws and regulations governing the handling of such personal information. This requirement stems from the need to balance the Federal Government's need to maintain information about individuals with the rights of individuals to be protected from unwarranted invasions of their privacy.

The IDA team conducted a literature review and interviewed a DoD privacy expert to produce this document, which provides an overview of the IDA team's initial research on applicable Federal laws and DoD issuances regarding the privacy rights of minors and the handling of PII that could impact potential tracking mechanisms that DoD might choose to recommend to Congress. The document aims to inform STEM education outreach program managers in DoD about the legal justifications and limitations related to establishing a Department-wide tracking system for student participation in its STEM outreach programs.

In the next chapter, we present a brief discussion of the legal definitions of the term "minor," and a review of Federal laws pertinent to the privacy concerns analyzed in this document. The third chapter presents DoD issuances providing guidance on compliance with Federal privacy laws. The final chapter presents a summary of the reviewed Federal laws and conclusions on the application of those laws to tracking minors.

2. Laws Governing Privacy Rights Relevant to Students and Minors

To produce the report required in subsection (c) of Section 1726, the legal implications of tracking minor students participating in DoD-funded STEM education programs must be identified and assessed. Therefore, the following sections of this chapter discuss the legal definitions of the term "minor," and pertinent Federal laws that help address this issue.

A. Definitions and Privacy Concerns of a "Minor"

A "minor" is defined as a person who is under the age of majority, when a person gains the legal status of an adult. Laws pertaining to minors in nearly all states demarcate the age of 18 as the base legal age, except for Alabama (19), Mississippi (21), and Nebraska (19).[8] Minors are generally afforded the basic rights granted by the United States Constitution, but some of their rights and responsibilities are limited and they need to be under the care of a parent or legal guardian. Although minors do not have all the legal rights of adults, they are afforded special protections and care by law to ensure their safety and well-being. Privacy matters require special considerations for minors because they are either developmentally immature or are precluded by law to make informed decisions for themselves.[9] A lengthier discussion on the legal definitions of a minor and the rights of minors appears in Appendix C.

A minor's right to privacy in the digital age further complicates the already complex issues surrounding privacy of minors. In their early years, the digital identities of minors are often shaped by others, when data related to a minor is generated and collected by their parents, schools, medical providers, and other entities such as websites.[10] Minors are not the creators of the content and have no control over the aggregation and use of such data at an age where they are unable to understand the consequences. "The primary concern, is that connecting all those data points creates a 'profiles' [*sic*] [of] the student that will follow

[8] "State Legal Ages Laws," FindLaw, accessed March 2021, https://statelaws.findlaw.com/family-laws/legal-ages.html.

[9] Grootens-Wiegers, Petronella et al., "Medical decision-making in children and adolescents: developmental and neuroscientific aspects," BMC Pediatrics, 2017, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5422908/.

[10] "How to Protect Our Kids' Data and Privacy," *Wired*, accessed March 2021, https://www.wired.com/story/protect-kids-data/.

[them] into adulthood."[11] Privacy advocates for minors fear that such profiles are not always accurate and may create possible adverse effects on a minor's life, such as compromising the physical safety and dignity of a minor or negatively affecting a minor's future prospects in education or employment.

In consideration of the special interests involved in the privacy of minors, several Federal laws govern their privacy rights by providing varying degrees of protection.

B. Pertinent Federal Privacy Laws

Privacy laws require basic standards for data collection, transmission, processing, and erasure. Three major Federal laws enacted specifically to protect the privacy of data related to minors are the Children's Online Privacy Protection Act (COPPA), the Protection of Pupil Rights Amendment (PPRA), and the Family Educational Rights and Privacy Act (FERPA). In addition, the Privacy Act of 1974 is another Federal law that establishes a code of fair information practices to protect all individuals regardless of age.

1. Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA),[12] enacted in 1998 and last amended in 2013, requires the Federal Trade Commission (FTC) to issue and enforce regulations concerning the online privacy of minors. COPPA gives parents and legal guardians control over the information that websites can collect from minors; however, it only protects minors under 13 years of age. The FTC explains that "younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information."[13] COPPA rules, however, only apply to information collected online from minors themselves; it does not cover information collected from adults that may pertain to minors.[14]

COPPA applies to operators of commercial and general audience websites and online services, including mobile apps and smart devices that could collect, use, or disclose

---

[11] "Protecting Your Child's Privacy," Uniting4Kids, accessed March 2021, https://www.uniting4kids.com/protecting-your-childs-privacy/.

[12] [15 U.S.C. Chapter 91, §6501 - §6508]

[13] "Complying with COPPA: Frequently Asked Questions - A Guide for Business and Parents and Small Entity Compliance Guide," Federal Trade Commission, accessed Match 2021, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[14] "Federal Laws Enabling Parents to Protect Their Children's Privacy: FERPA, PPRA and COPPA," Parent Coalition for Student Privacy, accessed March 2021, https://studentprivacymatters.org/ferpa_ppra_coppa/#COPPA.

information originating from minors under the age of 13. COPPA requires that operators of these websites and services must:[15]

- Post comprehensive privacy policies describing their information practices;
- Provide direct notice to parents and obtain verifiable parental consent;
- Give parents the choice of consenting to the collection and use of information, but prohibit the operator from disclosing that information to third parties;
- Provide parents access to their child's information to review and/or delete;
- Give parents the opportunity to prevent further use or collection of information;
- Maintain the confidentiality, security, and integrity of information, including taking reasonable steps to release information only to parties capable of maintaining its confidentiality and security;
- Retain personal information for only as long as is necessary to fulfill its purpose and delete the information using reasonable measures to protect from unauthorized access or use; and
- Not condition a minor's participation in an online activity on the minor providing more information than is reasonably necessary to participate in that activity.[16]

COPPA may have specific application to DoD's issue relating to tracking minors in the its STEM education outreach programs, because it applies to web-based services used by schools, such as homework help lines, individualized education modules, online research and organizational tools, and web-based testing services. COPPA allows schools to consent to the collection of information on the parents' behalf as long as it is limited to the educational context "for the use and benefit of the school, and for no other commercial purpose."[17] However, privacy advocates for minors have asserted that many schools fail to engage in due diligence and authorize data collection practices that parents find objectionable.[18] To address this concern, the FTC recommends, as a best practice, that schools consider making website and online service notices available to parents to allow

---

[15] "Complying with COPPA: Frequently Asked Questions - A Guide for Business and Parents and Small Entity Compliance Guide," Federal Trade Commission.

[16] "An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity," COPPA, §312.7.

[17] "Complying with COPPA: Frequently Asked Questions - A Guide for Business and Parents and Small Entity Compliance Guide," Federal Trade Commission.

[18] "Federal Laws Enabling Parents to Protect Their Children's Privacy: FERPA, PPRA and COPPA," Parent Coalition for Student Privacy.

them to review the personal information collected on their child and to ensure that operators delete the information once it is no longer needed for educational purposes.

2. Protection of Pupil Rights Amendment (PPRA)

The Protection of Pupil Rights Amendment (PPRA),[19] enacted in 1978 and last amended in 2001, requires that parents consent before their children participate in certain surveys and physical exams, as well as prior to the collection of information used for marketing purposes. PPRA is administered by the Department of Education (DoEd).

The law applies to a survey if it concerns one or more of the following eight protected areas (protected information survey) and if the survey is funded as part of a program administered by the DoEd:[20]

- Political affiliations or beliefs of the student or student's parent;
- Mental or psychological problems of the student or student's family;
- Sexual behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of others with whom respondents have close family relationships;
- Legally recognized privileged or analogous relationships, such as with lawyers, doctors, or ministers;
- Religious practices, affiliations, or beliefs of the student or student's parent; or
- Income, other than as required by law to determine program eligibility.

If a survey covering these protected areas is not funded by the DoEd, written parental consent is not required, but parents must still receive notice from schools and have the opportunity to opt their child out of responding to the survey.

PPRA also grants parents the right to receive notice as well as an opportunity to opt their child out of the following:

- Any non-emergency, invasive physical examination or screening required by a school as a condition of attendance, which is administered by the school, and is not necessary to protect the immediate health and safety of a student, except for those permitted under state law; and

---

[19] (20 U.S.C. §1232h; 34 CFR Part 98).

[20] U.S. Department of Education, Student Privacy Policy Office, Protection of Pupil Rights Amendment (PPRA), SPPO-21-01.

- Activities of a school involving collection, disclosure, or use of personal information collected from students for the purpose of marketing or sales or for distribution to others for that purpose.[21]

PPRA states that the rights transfer from the parents to the child when the student turns 18 years of age or becomes an emancipated minor[22] under applicable state law.

3. Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA),[23] enacted in November 1974 and last amended in October 2001, prohibits the disclosure of PII in student education records to third parties without parental consent. It applies to all educational institutions that receive funding from the DoEd. The consent requirement transfers from the parents to the child when the student turns 18 years of age. The rights included under FERPA are as follows:[24]

- Parents or eligible students[25] have the right to inspect the student's education records maintained by the school;
- Parents or eligible students have the right to request that a school correct records they believe to be inaccurate or misleading;
- Schools must have written consent from the parent or eligible student in order to release any information from a student's education record; however, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;

---

[21] U.S. Department of Education, Student Privacy Policy Office, PPRA, SPPO-21-01.

[22] Minors have a legal mechanism called *emancipation*, which allows them to gain the status of an adult. Each state has its own laws governing a minor's eligibility for emancipation and, depending on the state, emancipation can commonly be gained through judicial petition, marriage, or enlistment in military service.

[23] (20 U.S.C. §1232g; 34 CFR Part 99).

[24] "Family Educational Rights and Privacy Act (FERPA)," U.S. Department of Education, accessed March 2021, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[25] FERPA define an "eligible student" as someone who has reached the age of 18 or who is attending a postsecondary institution at any age. Once a student becomes an "eligible student," the rights afforded his or her parents under FERPA transfer to that student.

- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific state law.[26]

Furthermore, under FERPA, schools may disclose "directory information" without consent.[27] However, parents and eligible students must be notified of intended disclosures through public means, such as student handbooks, and must be given a reasonable period of time to opt out of directory information being disclosed to third parties. FERPA defines "directory information" as information in the student's education records that "would not generally be considered harmful or an invasion of privacy if disclosed."[28] DoEd further states that directory information includes:

- Student's name;
- Address;
- Telephone listing;
- Electronic mail address;
- Photograph;
- Date and place of birth;
- Major field of study;
- Dates of attendance;
- Grade level;
- Participation in officially recognized activities and sports;
- Weight and height (if a member of an athletic team);
- Degrees, honors, and awards received;
- The most recent educational agency or institution attended;

[26] (34 CFR §99.31).

[27] (34 CFR §99.37).

[28] "Frequently Asked Question - 5. What is 'Directory Information'?," U.S. Department of Education, accessed March 2021, https://www2.ed.gov/policy/gen/guid/fpco/faq.html#q4

- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records; and
- A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records.[29]

Privacy advocates for minors assert that many amendments to FERPA over the years have considerably weakened the protections originally afforded by the Act, allowing schools to share students' PII with third parties without notifying parents and eligible students or gaining their consent.[30] For instance, according to the legislative history of FERPA drafted by the Parent Coalition for Student Privacy, a non-profit initiative supporting stronger student privacy, the NDAA FY 2002[31] requires schools to provide directory-type information (students' names, addresses, and telephone listings) to military recruiters who request it.[32] The Coalition asserts that such a requirement in the NDAA is possible due to the exceptions stated in FERPA.

The DoEd states the following, which has proven to be controversial among privacy rights advocates, on the FERPA data sharing exception:

> "Educational institutions across the country rely on sharing data, often sharing student information with those outside the school or district in order to improve classroom instruction, to measure student outcomes, and [to] facilitate implementation of educational applications to evaluate the effectiveness of educational programs. While the general rule under FERPA is that personally identifiable information from education records cannot be disclosed without written consent, FERPA includes exceptions that permit data sharing under certain conditions with agencies, vendors, or individuals to conduct studies, audit or evaluate programs, enforce or comply with related Federal legal requirements, or in the case of [a response] to health or safety emergencies. In addition, in some circumstances, FERPA allows educational institutions to share [these data] with contractors, volunteers, or other individuals performing services for the educational institution. In many cases, written agreements [must be developed] to protect student data,

---

[29] "Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information," U.S. Department of Education, accessed March 2021, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html.

[30] "Federal Laws Enabling Parents to Protect Their Children's Privacy: FERPA, PPRA and COPPA," Parent Coalition for Student Privacy.

[31] Pub. L. 107-107, *National Defense Authorization Act for Fiscal Year 2002*, 115 Stat. 1112, December 28, 2001.

[32] Parent Coalition for Student Privacy, *Legislative History of Major FERPA Provisions*, p. 5.

and the requirements differ depending on the conditions and parties involved."[33]

In fact, the DoEd provides a "cheat sheet" for schools to understand the most commonly used exceptions to the FERPA written consent requirement. Figure 2-1 depicts an excerpt relevant to studies, audits, or evaluations from the DoEd's FERPA Exceptions Summary. The entire Summary sheet is in Appendix D.

[33] "Privacy and Data Sharing," U.S. Department of Education, accessed March 2021, https://studentprivacy.ed.gov/privacy-and-data-sharing.

Studies	Audit or Evaluation
Conditions that must be met	
1. The disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to a. Develop, validate, or administer predictive tests; b. Administer student aid programs; or c. Improve instruction. 2. An educational agency or institution may disclose PII from education records, and a "FERPA-permitted entity" may redisclose PII only if a. The disclosing educational entity enters into a written agreement with the organization;	1. The disclosure of PII from education records must be to a. Audit or evaluate a Federal- or State-supported education program; or b. Enforce or comply with Federal legal requirements related to the program. 2. The receiving entity must be a State or local educational authority or other FERPA-permitted entity or must be an authorized representative of a State or local educational authority or other FERPA-permitted entity. 3. The party disclosing the PII from education records a. Must enter into a written agreement to designate anyone other than its employee as its authorized representative (each new audit, evaluation, or enforcement effort requires an agreement); and b. Is responsible for using reasonable methods to ensure to the greatest extent practicable that the authorized representative i. Uses the PII only for the authorized purpose; ii. Protects the PII from further unauthorized disclosures or other uses; and
b. The study does not permit identification of individual parents and students by anyone other than representatives of the organization with legitimate interests in the information; and c. The information is destroyed when no longer needed for the study purposes.	iii. Destroys the PII when no longer needed for the authorized purpose and in accordance with any specified time period set forth in a written agreement. 4. State and local educational authorities and other FERPA-permitted entities may redisclose the PII on behalf of the educational agency or institution. In particular, a. The disclosure must meet the requirements of an exception to consent in § 99.31 and either the educational agency or institution or other FERPA-permitted entity has complied with the recordkeeping requirements. 5. Authorized representatives of the FERPA-permitted entities may only redisclose the PII when expressly authorized in the parties' written agreement (assuming that the redisclosure by the authorized representative on behalf of the FERPA-permitted entity would be permissible under FERPA).

Figure 2-1. Excerpt of the FERPA Exceptions Summary

The full summary, created by DoEd's Privacy Technical Assistance Center (PTAC), is designed to assist state and local educational agencies (SEAs and LEAs) and other educational institutions in determining the conditions under which FERPA permits the disclosure, without consent, of PII from education records to third parties such as researchers, contractors, volunteers, and journalists. The disclosure must meet one or more of the conditions outlined in FERPA and its regulations.[34] The PTAC summary provides a high-level overview of the four most commonly used exceptions to the FERPA written consent requirement, including applicable recording requirements.[35]

Therefore, if DoD were to require student PII as part of an effort to track students participating in DoD-supported STEM education programs that partner with DoEd-funded educational institutions, the burden is on the educational institutions administering the programs to determine the exceptions under which such disclosure without consent is permitted, or to obtain consent if deemed necessary.

4. Privacy Act

The Privacy Act, enacted in December 1974,[36] regulates the collection, maintenance, use, and dissemination of PII by executive branch agencies. The Privacy Act makes no age delineations regarding the handling of PII.

The Act's general disclosure prohibition states, "no agency shall disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[37] This clause is known as the "No Disclosure without Consent" Rule. The prohibition is subject to 12 exceptions, listed below, when the disclosure would be:

1. To those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties (5 U.S.C. § 552a(b)(1));
2. Required under section 552 of the Freedom of Information Act (5 U.S.C. § 552a(b)(2));

---

[34] 20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31.

[35] U.S. Department of Education, Privacy Technical Assistance Center, *FERPA Exceptions Summary,* PTAC-Handout-2H, April 2014.

[36] (5 U.S.C. § 552a).

[37] "Overview of the Privacy Act: 2020 Edition – Conditions of Disclosure to Third Parties," U.S. Department of Justice, accessed March 2021, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties#consentrules.

3. For a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) (5 U.S.C. § 552a(b)(3));
4. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13 (5 U.S.C. § 552a(b)(4));
5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable (5 U.S.C. § 552a(b)(5));
6. To the National Archives and Records Administration as a record that has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value (5 U.S.C. § 552a(b)(6));
7. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency that maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought (5 U.S.C. § 552a(b)(7));
8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual (5 U.S.C. § 552a(b)(8));
9. To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee (5 U.S.C. § 552a(b)(9));
10. To the Comptroller General, or an authorized representative thereof, in the course of the performance of the duties of the Government Accountability Office (5 U.S.C. § 552a(b)(10));
11. Pursuant to the order of a court of competent jurisdiction (5 U.S.C. § 552a(b)(11)); and

12. To a consumer reporting agency in accordance with section 3711(e) of Title 31 (5 U.S.C. § 552a(b)(12)).[38]

A system of records (SOR) is a group of records, controlled by Federal agencies or their components, in which information is stored and can be retrieved by the name of an individual, identification number, or other unique identifier assigned to that individual.[39]

To store and retrieve PII from a SOR, the Privacy Act requires Federal agencies to publish a system of records notice (SORN) in the Federal Register. A SORN aims to inform the public of the existence of the system or records and to provide notice of an individual's rights under the Privacy Act for accessing and correcting information maintained in the SOR pertaining to themselves. Specifically related to minors, the Act states that "the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual."[40] The Act requires each Federal agency that maintains a SOR to maintain only such information about an individual that is relevant and necessary to accomplish a purpose stemming from a statute or an executive order of the President.

The Act permits the collection and retrieval of PII as long as a Privacy Act Statement (PAS) is provided to the individual, or a parent in the case of minors, at the point of collection. The PAS explains why the information is being collected and how the information will be used. Although the disclosure of information is voluntary, the PAS can state how non-disclosure may impact the benefits the individual may receive from the activity in which they are participating.

---

[38] "Overview of the Privacy Act: 2020 Edition – Twelve Exceptions to the 'No Disclosure without Consent Rule'," U.S. Department of Justice, accessed March 2021, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties#exceptions.

[39] "About SORNs: System of Records Notices," Defense Privacy, Civil Liberties, and Transparency Division, U.S. Department of Defense, accessed March 2021, https://dpcld.defense.gov/Privacy/SORNs/.

[40] (5 U.S.C. § 552a, (h)).

3. Department of Defense Issuances on Privacy

DoD's Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) in the Office of the Secretary of Defense implements the Department's Privacy and Civil Liberties programs through advice, monitoring, official reporting, and training.[41] The Division provides a useful summary of authorities and guidance related to privacy issues at within DoD.

A. DoD Issuances on Privacy

According to the DPCLTD, three DoD issuances address privacy issues:

- DoDI 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019;
- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007; and
- DoDI 1000.30, "Reduction of Social Security Number (SSN) Use within DoD" August 1, 2012.

Although none of the issuances listed above makes any reference to the privacy rights of minors specifically relevant to answering DoD's issue on the tracking mechanism explored in this document,[42] DoDI 5400.11 does state that, under Privacy Act requirements, all DoD Components will:

- Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII maintained in a system of records to that which is legally authorized, relevant, and reasonably deemed necessary to accomplish a DoD function;
- Maintain all records with PII in accordance with applicable records retention or disposition schedules approved by the National Archives and Records Administration; and
- Impose conditions, where appropriate, when sharing PII with other Federal and non-Federal agencies or entities (including the selection and implementation of particular security and privacy controls) that govern the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of the

[41] "About the Office: Privacy Program," Defense Privacy, Civil Liberties, and Transparency Division, U.S. Department of Defense, accessed March 2021, https://dpcld.defense.gov/Privacy/About-the-Office/.

[42] DoD 5400.11-R does outline restrictions with regard to accessing medical records of minors.

PII. This will be accomplished using written agreements, including contracts, data use agreements, information exchange agreements, and memoranda of understanding when appropriate.[43]

DoDI 5400.11 also states that under the authority, direction, and control of the Director, Administration and Management (DA&M), the Director of the Directorate for Oversight and Compliance (DO&C) will manage "privacy risks associated with any DoD activities that involve the creation, collection, use, process, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems."

DoDI 5400.11 further requires that the Chief of the DPCLTD, under the authority, direction, and control of the Director, DO&C, must:

- Review legislative, regulatory, and other policy proposals with privacy and civil liberties implications, including those relating to how DoD maintains its PII, as well as proposed testimony in accordance with DoDD 5500.01; and
- Provide guidance, assistance, and support to DoD Components in their implementation of DoD Privacy and Civil Liberties Programs to ensure that all requirements developed to maintain PII conform to DoD Privacy and Civil Liberties Programs standards.[44]

B. DoD Guidance on the Privacy Act

The DPCLTD also provides guidance on the rights of minors under the Privacy Act. The DPCLTD cites a memorandum communicating an advisory opinion by the Defense Privacy Board affirming that minors have the same rights and protections as adults do under the Privacy Act:

> "The Privacy Act provides that "the parent of any minor . . . may act on behalf of the individual." 5 U.S.C. § 552a(h). This subsection ensures that minors have a means of exercising their rights under the Privacy Act. Office of Management and Budget Privacy Act Guidelines (OMB Guidelines), 40 Fed. Reg. 28949, 28970 (July 9, 1975). It does not preclude minors from exercising rights on their own behalf, independent of any parental exercise. Parental exercise of the minor's Privacy Act rights is discretionary. A Department of Defense (DoD) component may permit parental exercise of a minor's Privacy Act rights at its discretion, but the parent has no absolute right to exercise the minor's rights absent a court order or the minor's consent. See OMB Guidelines, 40 Fed. Reg. 56741, 56742 (December 4, 1975). Further, the parent exercising a minor's rights under the Privacy Act

[43] DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, January 29, 2019, pp. 3-4.

[44] DoDI 5400.11, p. 7.

must be doing so on behalf of the minor and not merely for the parent's benefit. DePlanche v. Califano, 549 F. Supp. 685 (W.D. Mich. 1982)."[45]

Regarding the PAS required by the Privacy Act, DoD 5400.11-R states that:

"When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act statement is required regardless of the medium used to collect the information…The statement enables the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any system of records."[46]

Elements that make up a PAS include:

- The Federal statute or Executive Order that authorizes collection of the requested information;
- The principal purpose or purposes for which the information is to be used;
- The routine uses that will be made of the information;
- Whether providing the information is voluntary or mandatory; and
- The effects on the individual if they choose not to provide the requested information.[47]

To expand on the full meaning of the final two bulleted points, the PAS can be written in a manner that such a disclosure would be conditional. In other words, while an individual may participate in an activity, the decision not to disclose information may mean that they would not receive the full benefits of the program.

C. DoD System of Records Notice on Defense Training Records

Following Privacy Act requirements on SORs, DoD publishes SORNs in the Federal Register. Until recently, DoD Components have published individual SORNs for the various systems of records under the individual Components' control. In a bid to consolidate and minimize the proliferation of SORNs, DPCLTD has undertaken an effort to publish "umbrella" SORNs or DoD-wide SORNs for systems of record across DoD that have a common function or purpose.

---

[45] The Judge Advocate General's School, U.S. Army, JA 235, Government Information Practices--Casebook, Appendix A (March 2000), p. A-15.

[46] DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, p. 19.

[47] DoD 5400.11-R, pp. 19-20.

One such DoD-wide SORN is DoD 0005, published in December 2020, which applies to all systems of record containing the information of individuals participating in the numerous defense training programs in DoD.[48] As described in the SORN, DoD 0005 applies to systems of records that:

1. Support DoD training as may be required by law and policy, as well as for mission, professional development, and employment purposes.
2. Track individual training and professional development, including enrollment, participation and completion information, class schedules, programs, and instructors.
3. Track training and professional development trends and needs, testing and examination materials, credentialing, promotional decisions, career development planning, and assessments of professional competencies and training efficacy.
4. Determine eligibility for enrollment/attendance, and facilitate post-training job referrals and placement.
5. Monitor and track the expenditure of training and related travel funds and training-related contract management.
6. Facilitate the compilation of statistical information about training.
7. Fulfill regulatory requirements to report civilian employee training to the Office of Personnel Management.

The SORN states that record source categories include "other federal government learning and student management systems, such as the Department of Education Postsecondary Education Participants System (PEPS), and State Departments of Education and their grant recipients." See Appendix E for the contents of the entire DoD 0005 SORN.

Ms. Viki Halabuk, a Senior Privacy Management Analyst in the DPCLTD Directorate for Oversight and Compliance, suggested that, given the potential commonalities involved in systems for personnel records for DoD training programs, SORN DoD 0005 might be leveraged to create a potential tracking mechanism to meet the requirements of Section 1726.[49] If DoD were to establish a system of records to store and retrieve the PII of students to track their participation in DoD-sponsored STEM outreach programs, a SORN similar to DoD 0005 would be necessary.

---

[48] Defense Training Records, DoD 0005. (December 28, 2020; 85 FR 84316), accessed March 12, 2021, https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DoD-0005.pdf.

[49] Discussion between IDA and Ms. Viki Halabuk, Senior Privacy Management Analyst, DPCLTD, Directorate for Oversight and Compliance, March 12, 2021.

4. Summary of Laws and Conclusions

A. Summary of Pertinent Laws

Table 4-1 summarizes all privacy-related laws relevant to this research.

Table 4-1. Summary of Pertinent Federal Laws

COPPA	• Issues and enforces regulations concerning the online privacy of minors by giving parents control over the information that websites can collect from minors. • Protects minors under 13 years of age. • Applies to operators of commercial and general audience websites and online services, which includes mobile apps and smart devices. • Applies to web-based services used by schools such as homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. • Allows schools to consent to the collection of information on the parents' behalf as long as it is limited to the educational context. • Prohibits operators from conditioning a minor's participation in an online activity on the minor providing more information than is reasonably necessary to participate in that activity.
PPRA	• Requires parents to consent before their children participate in certain surveys, certain physical exams, and the collection of information used for marketing purposes. • Applies to a survey if it concerns one or more of eight protected information areas (protected information survey).
FERPA	• Prohibits the disclosure of PII in student education records to third parties without parental consent. • Applies to all educational institutions that receive funding from the DoEd. • Schools may disclose "directory information" (which includes information (students' names, addresses, and telephone listings) without consent.

	• Includes exceptions that permit data sharing under certain conditions with agencies, vendors, or individuals to conduct studies, audit or evaluate programs, and enforce or comply with related Federal legal requirements. • DoEd provides a "cheat sheet" for schools to understand the most commonly used exceptions to the FERPA written consent requirement. • Burden of obtaining consent is on the educational institutions receiving DoEd funding.
Privacy Act	• Regulates the collection, maintenance, use, and dissemination of PII by Federal executive branch agencies. • Makes no age delineations regarding the handling of PII. • Requires Federal agencies to publish a SORN in the Federal Register prior to storing and retrieving PII from a SOR. • Permits the collection and retrieval of PII, as long as a PAS is provided to the individual, or a parent in the case of minors, at the point of collection. • A PAS states how non-disclosure of information may impact the benefits the individual may receive from the activity in which they are participating.

B. Conclusions

NDAA FY 2021 Section 1726(c)(2)(C) requires DoD to recommend mechanisms to track student participation across its cyber-related education outreach programs; however, because such programs include students who are minors, tracking minors is a complicated legal issue due to concerns about minors' privacy rights. Before tracking minor students, DoD must assure that it is lawful to use their PII to track them for the purposes described by Congress, and then, if allowed, DoD must determine how to do so while complying with all privacy-related laws.

Based on its analysis of pertinent Federal laws, the IDA research team has assessed that the PII of minors may be used for the tracking purposes described in Section 1726 of the FY2021 NDAA, so long as DoD organizations comply with applicable federal laws and DoD policies, including those addressed in this document, and subject to prior review and concurrence by cognizant DoD counsel. FERPA permits, under certain conditions, the disclosure of students' PII from education records. In any DoD STEM education outreach program that partners with DoEd-funded educational institutions, the burden is on such institutions to ascertain the need for consent, to obtain it if deemed necessary, and to share the PII required for the tracking mechanism.

The Privacy Act also permits the collection of PII, regardless of age of the student, as long as a PAS asking for consent is provided to the individual, or parent in the case of

minors. The PAS informs recipients about the reason the information is being collected, and what will be done with the information. While the disclosure of information is voluntary, the PAS can state how a decision to not disclose information may impact the benefits the individual may receive from the activity in which they are participating.

Appendix A.
NDAA FY 2021 Section 1726

The National Defense Authorization Act for Fiscal Year 2021 Section 1726 (NDAA FY 2021) details requirements regarding DoD cyber workforce efforts. Specifically, subsection (c) concerning the alignment of cyber security training programs directs the Secretary of Defense to submit to the congressional defense committees a report "containing recommendations on how cyber security training programs described in section 1649 of the National Defense Authorization Act for Fiscal Year 2020 can be better aligned and harmonized."[50]

In Section 1726, Congress directs the Secretary of Defense to take into consideration "existing Federal childhood cyber education programs," including the programs identified in NDAA FY 2020 Section 1649, when completing the report. Furthermore, one requirement of the report is to provide recommendations concerning "mechanisms for tracking participation and transition of participation from one such program to another."[51]

The following four pages present the full text of Section 1726 and the sections relevant to the issue discussed in this document are highlighted in yellow.

[50] Pub. L. 116-283, *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, January 1, 2021, p. 1875.

[51] Pub. L. 116-92, *National Defense Authorization Act for Fiscal Year 2020*, 133 Stat. 1758, December 20, 2019.

One Hundred Sixteenth Congress
Of The
United States of America

AT THE SECOND SESSION

SEC. 1726. DEPARTMENT OF DEFENSE CYBER WORKFORCE EFFORTS

(a) RESOURCES FOR CYBER EDUCATION.—

(1) IN GENERAL.—The Chief Information Officer of the Department of Defense, in consultation with the Director of the National Security Agency (NSA), shall examine the current policies permitting National Security Agency employees to use up to 140 hours of paid time toward NSA's cyber education programs.

(2) REPORT.—

(A) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees and the congressional intelligence committees a strategy for expanding the policies described in paragraph (1) to—

(i) individuals who occupy positions described in section 1599f of title 10, United States Code; and

(ii) any other individuals who the Chief Information Officer determines appropriate.

(B) IMPLEMENTATION PLAN.—The report required under subparagraph (A) shall detail the utilization of the policies in place at the National Security Agency, as well as an implementation plan that describes the mechanisms needed to expand the use of such policies to accommodate wider participation by individuals described in such subparagraph. Such implementation plan shall detail how such individuals would be able to connect to the instructional and participatory opportunities available through the efforts, programs,

initiatives, and investments accounted for in the report required under section 1649 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), including the following programs:

(i) GenCyber.

(ii) Centers for Academic Excellence – Cyber Defense.

(iii) Centers for Academic Excellence – Cyber Operations.

(C) DEADLINE.—Not later than 120 days after the submission of the report required under subparagraph (A), the Chief Information Officer of the Department of Defense shall carry out the implementation plan contained in such report.

(b) IMPROVING THE TRAINING WITH INDUSTRY PROGRAM.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Principal Cyber Advisor of the Department of Defense, in consultation with the Principal Cyber Advisors of the military services and the Under Secretary of Defense for Personnel and Readiness, shall submit to the Secretary of Defense and the congressional defense committees a review of the current utilization and utility of the Training With Industry (TWI) programs, including relating to the following:

(A) Recommendations regarding how to improve and better utilize such programs, including regarding individuals who have completed such programs.

(B) An implementation plan to carry out such recommendations.

(2) ADDITIONAL.—Not later than 90 days after the submission of the report required under paragraph (1), the Secretary of Defense shall carry out such elements of the implementation plan required under paragraph (1)(B) as the Secretary considers appropriate and notify the congressional

defense committees of the determinations of the Secretary relating thereto.

(c) ALIGNMENT OF CYBERSECURITY TRAINING PROGRAMS.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report containing recommendations on how cybersecurity training programs described in section 1649 of the National Defense Authorization Act for Fiscal Year 2020 can be better aligned and harmonized.

(2) REPORT.—The report required under paragraph (1) shall provide recommendations concerning the following topics and information:

(A) Developing a comprehensive mechanism for utilizing and leveraging the Cyber Excepted Service workforce of the Department of Defense referred to in subsection (a), as well as mechanisms for military participation.

(B) Unnecessary redundancies in such programs, or in any related efforts, initiatives, or investments.

(C) Mechanisms for tracking participation and transition of participation from one such program to another.

(D) Department level oversight and management of such programs.

(3) CYBER WORKFORCE PIPELINE AND EARLY CHILDHOOD EDUCATION.—

(A) ELEMENTS.—The Secretary of Defense shall, when completing the report required under paragraph (1), take into consideration existing Federal childhood cyber education programs, including the programs identified in the report required under section 1649 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) and the Department of Homeland Security's Cybersecurity Education and Training Assistance Program(CETAP), that

can provide opportunities to military-connected students and members of the Armed Forces to pursue cyber careers.

(B) DEFINITION.—In this paragraph, the term "military-connected student" means an individual who—

(i) is a dependent a member of the Armed Forces serving on active duty; and

(ii) is enrolled in a preschool, an elementary or secondary school, or an institution of higher education.

Appendix B.
NDAA FY 2020 Section 1649

The National Defense Authorization Act for Fiscal Year 2021 Section 1726 (NDAA FY 2021 §1726) details requirements regarding DoD cyber workforce efforts. Specifically, subsection (c) concerning the alignment of cyber security training programs directs the Secretary of Defense to submit to the congressional defense committees a report "containing recommendations on how cyber security training programs described in section 1649 of the National Defense Authorization Act for Fiscal Year 2020 can be better aligned and harmonized."[52] NDAA FY 2020 Section 1649 refers to DoD's "efforts, programs, initiatives, and investments to train elementary, secondary, and postsecondary students in fields related to cybersecurity, cyber defense, and cyber operations."[53]

In NDAA FY 2021 Section 1726, Congress directs the Secretary of Defense to take into consideration "existing Federal early childhood cyber education programs," including the programs identified in NDAA FY 2020 Section 1649, when completing the report.

The next page presents the full text of Section 1649.

[52] Pub. L. 116-283, *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, January 1, 2021, p. 1875.

[53] Pub. L. 116-92, *National Defense Authorization Act for Fiscal Year 2020*, 133 Stat. 1758, December 20, 2019.

Public Law 116-92

One Hundred Sixteenth Congress
Of The
United States of America

SEC. 1649. REPORT ON CYBERSECURITY TRAINING PROGRAMS.

Not later than 240 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate a report that accounts for all of the efforts, programs, initiatives, and investments of the Department of Defense to train elementary, secondary, and postsecondary students in fields related to cybersecurity, cyber defense, and cyber operations. The report shall—

(1) include information on the metrics used to evaluate such efforts, programs, initiatives, and investments, and identify overlaps or redundancies across the such efforts, programs, initiatives, and investments; and

(2) address how the Department leverages such efforts, programs, initiatives, and investments in the recruitment and retention of both the civilian and military cyber workforces.

Appendix C.
Definitions and Rights of a "Minor"

The age of majority is reached when a person gains the legal status of an adult. A "minor" is defined as a person who is under the age of majority, which can vary depending on jurisdiction and application. Laws pertaining to minors in nearly all states demarcate the age of 18 as the base legal age, except for Alabama (19), Mississippi (21), and Nebraska (19).[54] However, minors do have a legal mechanism called *emancipation*, which allows them to gain the status of an adult. Each state has its own laws governing a minor's eligibility for emancipation and, depending on the state, emancipation can commonly be gained through judicial petition, marriage, or enlistment in military service.[55]

Minors are generally afforded the basic rights granted by the U. S. Constitution, but some of their rights and responsibilities are limited, and they need to be under the care of a parent or legal guardian. For instance, minors cannot typically enter into legally binding contracts or consent to medical treatment; however, each state has its own exceptions where minors are granted the rights to make decisions in certain areas of their life. The age of majority is a distinct legal concept from the "age of license," which is a legally enforceable right or privilege to participate in certain activities such as voting, drinking alcohol, or driving.[56] The age of license does not necessarily coincide with the age of majority and can vary by activity and jurisdiction.

Although minors do not have all the legal rights of an adult, they are afforded special protections and care by law to ensure their safety and well-being. For certain legal purposes, minors are treated differently in areas such as punishment in criminal matters, hours and types of employment, and privacy of personal records.

---

[54] "State Legal Ages Laws," FindLaw, accessed March 2021, https://statelaws.findlaw.com/family-laws/legal-ages.html.

[55] "Legal age," Legal Information Institute, Cornell Law School, accessed March 2021, https://www.law.cornell.edu/wex/legal_age.

[56] "Legal age," Legal Information Institute, Cornell Law School.

The U.S. Constitution, particularly the Fourth Amendment,[57] provides the principal basis for establishing that an individual has a legitimate expectation of privacy. Although it is not explicitly found in the Constitution, the constitutional right to privacy was established in a landmark decision by the U. S. Supreme Court in *Griswold v. Connecticut*. Justice William Douglas wrote for the majority that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance…Various guarantees create zones of privacy."[58] In the case of minors, privacy matters require special considerations because minors are either developmentally immature[59] or are precluded by law to make informed decisions for themselves. Developmental psychologists contend that a minor's sense of privacy is important in "fostering personal identity, encouraging competence, and promoting security and trust by the minor."[60]

---

[57] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." – "Fourth Amendment, Constitution of the United States," Constitution Annotated, access April 2021, https://constitution.congress.gov/constitution/amendment-4/.

[58] "Estelle T. Griswold et al. Appellants, v. State of Connecticut," Legal Information Institute, Cornell Law School, accessed April 20, 2021, https://www.law.cornell.edu/supremecourt/text/381/479.

[59] Grootens-Wiegers, Petronella, et al. *Medical Decision-Making in Children and Adolescents: Developmental and Neuroscientific Aspects*.

[60] Henning, Kristen, *The Fourth Amendment Rights of Children at Home: When Parental Authority Goes Too Far*, Georgetown University Law Center, 2011, p. 89.

Appendix D.
FERPA Exceptions Summary

Figure D-1 and Figure D-2 depict the document created by the DoEd's PTAC to assist SEAs, LEAs, and other educational institutions to determine under what conditions FERPA permits the disclosure, without consent, of PII from education records to third parties, such as researchers, contractors, volunteers, and journalists.[61]

FERPA permits an educational agency or institution to disclose PII from an education record of a student without the consent of a parent or eligible student if the disclosure meets one or more of the conditions outlined in 20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31. What follows is a high-level overview provided by PTAC of the four most commonly used exceptions to the FERPA written consent requirement, including applicable recording requirements.

[61] U.S. Department of Education, Privacy Technical Assistance Center, "FERPA Exceptions Summary," PTAC-Handout-2H, April 2014.

FERPA Exceptions—Summary

Privacy Technical Assistance Center

This Privacy Technical Assistance Center (PTAC) document is designed to assist State and local educational agencies (SEAs and LEAs) and educational institutions with determining under what conditions the Family Educational Rights and Privacy Act (FERPA) permits the disclosure of personally identifiable information (PII) from education records to third parties, such as researchers, contractors, volunteers, and journalists.

Generally, FERPA requires written consent from parents or "eligible students" (students who are at least 18 years of age or attending a postsecondary institution) in order to release PII from education records. In the absence of the written consent, FERPA permits an educational agency or institution to disclose PII from an education record of a student if the disclosure meets one or more of the conditions outlined in 20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31. Below is a high-level overview of the four most commonly used exceptions to the FERPA written consent requirement, including applicable recordation requirements. For a more detailed explanation of these and other FERPA exceptions, please visit https://studentprivacy.ed.gov.

Directory Information*	School Official (Schools and LEAs only)	Studies	Audit or Evaluation
Conditions that must be met			
1. A school and/or LEA must properly designate "directory information": a. Directory information may only include PII that is generally not considered harmful or an invasion of privacy if disclosed. b. The policy must clearly detail the types of PII that have been designated as directory information, the parent's or eligible student's right to refuse to let any or all of these types of PII be designated as directory information, and the period of time that the parent or eligible student has to opt out of such a disclosure of directory information.	1. A school and/or LEA must a. Establish criteria in the annual notification of FERPA rights about who is a "school official" and what constitutes a "legitimate educational interest"; b. Determine that the disclosure is to a school official who has a legitimate educational interest in the education records; and c. Use reasonable methods to ensure that school officials obtain access to only those education records in which they have a legitimate educational interest.	1. The disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to a. Develop, validate, or administer predictive tests; b. Administer student aid programs; or c. Improve instruction. 2. An educational agency or institution may disclose PII from education records, and a "FERPA-permitted entity" may redisclose PII only if a. The disclosing educational entity enters into a written agreement with the organization;	1. The disclosure of PII from education records must be to a. Audit or evaluate a Federal- or State-supported education program; or b. Enforce or comply with Federal legal requirements related to the program. 2. The receiving entity must be a State or local educational authority or other FERPA-permitted entity or must be an authorized representative of a State or local educational authority or other FERPA-permitted entity. 3. The party disclosing the PII from education records a. Must enter into a written agreement to designate anyone other than its employee as its authorized representative (each new audit, evaluation, or enforcement effort requires an agreement); and b. Is responsible for using reasonable methods to ensure to the greatest extent practicable that the authorized representative i. Uses the PII only for the authorized purpose; ii. Protects the PII from further unauthorized disclosures or other uses; and

* *While FERPA does not require that schools implement a directory information policy, if they do so, certain conditions must be met.*

Figure D-1. FERPA Exceptions Summary – Page 1 of 2

Directory Information	School Official (Schools and LEAs only)	Studies	Audit or Evaluation
2. A school and/or LEA must give a public notice to parents of students in attendance and eligible students in attendance prior to disclosing directory information. 3. Subject to a few exceptions, parents or eligible students must not have opted out of the disclosure of directory information.	2. If outsourcing institutional services or functions to a third party, outside parties may be considered "school officials" if the outside party a. Performs an institutional service or function for which the school would otherwise use employees; b. Is under the direct control of the school with respect to the use and maintenance of education records; and c. Complies with the PII from education records use and redisclosure requirements.	b. The study does not permit identification of individual parents and students by anyone other than representatives of the organization with legitimate interests in the information; and c. The information is destroyed when no longer needed for the study purposes.	iii. Destroys the PII when no longer needed for the authorized purpose and in accordance with any specified time period set forth in a written agreement. 4. State and local educational authorities and other FERPA-permitted entities may redisclose the PII on behalf of the educational agency or institution. In particular, a. The disclosure must meet the requirements of an exception to consent in § 99.31 and either the educational agency or institution or other FERPA-permitted entity has complied with the recordkeeping requirements. 5. Authorized representatives of the FERPA-permitted entities may only redisclose the PII when expressly authorized in the parties' written agreement (assuming that the redisclosure by the authorized representative on behalf of the FERPA-permitted entity would be permissible under FERPA).
Legal references			
34 CFR §§ 99.3, 99.31(a)(11), and 99.37.	34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii).	34 CFR § 99.31(a)(6).	34 CFR §§ 99.31(a)(3) and 99.35.
Other notes			
Recordation: FERPA does not require educational agencies and institutions to record disclosures of appropriately designated directory information (§ 99.32(d)(4)).	*Recordation*: FERPA (§ 99.32(d)(2)) does not require educational agencies and institutions to record disclosures of PII from education records to school officials under § 99.31(a)(1).	*Recordation*: FERPA requires educational agencies and institutions to record all disclosures of PII from education records to organizations made under the studies exception (§ 99.32).	*Recordation*: FERPA requires educational agencies and institutions to record all disclosures of PII from education records made under the audit or evaluation exception (§ 99.32). ➢ State and local educational authorities (and other FERPA-permitted entities listed in § 99.31(a)(3)) redisclosing PII on behalf of the educational agency or institution must record disclosures according to the requirements in § 99.32(b)(2).

See PTAC website for Additional Resources and Glossary: https://studentprivacy.ed.gov

Figure D-2. FERPA Exceptions Summary – Page 2 of 2

Appendix E.
DoD 0005: System of Records Notice

The SORN numbered DoD 0005, published in December 2020 by DoD's DPCLTD, is presented in Figure E-1 through Figure E-7. This SORN addresses DoD-wide requirements for compliance with the Privacy Act of 1974 for records maintained on individuals participating in DoD training programs. Elements of this SORN may be beneficial to developing a SORN for the tracking of students across DoD STEM programs.[62]

[62] Defense Training Records, DoD 0005. (December 28, 2020; 85 FR 84316), accessed March 12, 2021, https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DoD-0005.pdf.

SYSTEM NAME AND NUMBER: Defense Training Records, DoD 0005. (December 28, 2020; 85 FR 84316)

SECURITY CLASSIFICATION: Classified and unclassified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations, at which electronic or paper training records may be maintained. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): The system managers are as follows:

A. Program Manager, Advanced Distributed Learning Initiative, Office of the Assistant Secretary of Defense for Readiness, 4000 Defense Pentagon, Washington, DC 20301-4000, whs-mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil.

B. Commander, Air Education and Training Command (AETC), Joint Base San Antonio-Randolph, TX, (703) 693-2735.

C. Commander, U.S. Army Training Support Center (USATSC), 1900 Jackson Lane, Fort Eustis, VA 23604-5166, (571) 515-0306.

D. Executive Director, Naval Education and Training Command (NETC), Learning and Development, 250 Dallas Street, Pensacola, FL 32508, donfoia-pa@navy.mil.

E. Commanding General, United States Marine Corps, Training and Education Command (TECOM), 1019 Elliot Road, Quantico, VA 22134-5010, (703) 614-4008.

For Combatant Commands, or other Defense Agencies, the system manager can be found at: www.FOIA.gov under the DoD component with oversight of the records.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. Chapter 41, Training; 5 CFR part 410, Office of Personnel Management-Training; E.O. 11348, Providing for the Further Training of Government Employees, as amended by E.O. 12107, Relating to the Civil Service Commission and Labor-Management in the Federal Service; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1746 Defense Acquisition University; 10 U.S.C.1747, Acquisition Fellowship Program; DoD Instruction 1215.08 Senior Reserve Officers Training Corp Programs; DoD Directive 1322.18, Military Training; DoD Directive 1322.08E, Voluntary Education Programs for Military Personnel; DoD Instruction 1322.26, Distributed Learning; DoD Instruction 1322.25, Voluntary Education Program; DoD Instruction 1322.9, Job Training, Employment Skills Training, Apprenticeships, and Internships (JTEST-AI) for Eligible Service Members; DoD Instruction 1430.16, Growing Civilian Leaders; DoD Instruction 5132.13, Staffing of Security Cooperation Organizations (SCOs) and the Selection and Training of Security Cooperation Personnel; DoD Instruction 1215.21, Reserve Component (RC) Use of Electronic-based Distributed Learning; Directive-Type Memorandums 13-004, Operation of the DoD Financial Management

Figure E-1. Defense Training Records SORN, DoD 0005 – Page 1 of 7

Certification Program Methods for Training; and DoD Instruction 1015.2, Military Morale, Welfare and Recreation (MWR), DoD Instruction 1300.26, Operation of the DoD Financial Management Certification Program; and E.O. 9397.

PURPOSE(S) OF THE SYSTEM:

a. To support DoD training as may be required by law and policy, as well as for mission, professional development, and employment purposes.

b. To track individual training and professional development, including enrollment, participation and completion information; and class schedules, programs, and instructors.

c. To track training and professional development trends and needs, testing and examination materials, credentialing, promotional decisions, career development planning, and assessments of professional competencies and training efficacy.

d. To determine eligibility for enrollment/attendance, and facilitate post-training job referrals and placement.

e. To monitor and track the expenditure of training and related travel funds, and training-related contract management.

f. To facilitate the compilation of statistical information about training.

g. To fulfill regulatory requirements to report civilian employee training to the Office of Personnel Management.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DoD-affiliated individuals enrolled in training sponsored or administered by DoD, including: Military Service members (active duty, Guard/Reserve, cadets and midshipmen, Public Health Services, and the Coast Guard personnel when operating as a Military Service with the Navy), DoD civilian employees (including non-appropriated fund employees and DoD Outside the Contiguous United States hires, also known as local national employees), dependents and family members of the above, contractors, personnel of other government agencies, and other individuals affiliated with the DoD.

CATEGORIES OF RECORDS IN THE SYSTEM:

a. Personal information, such as name, Social Security number (SSN), DoD ID Number, or other DoD assigned student or educational ID number, date and place of birth, gender, citizenship, driver's license, photograph, email address(es), personal and duty phone numbers, emergency contact information, race and ethnic origin, religious preference collected to support the placement of chaplain at appropriate locations.

b. Employment information, such as employment status, duty position, service component, branch, personnel classification, security clearance, grade/rank/series, military status, military occupational specialty, official orders, unit of assignment, occupation, and other organizational affiliation information.

Figure E-2. Defense Training Records SORN, DoD 0005 – Page 2 of 7

c. Select Personal Health Information, such as medical profiles, physical examinations, psychological test record for special assignment eligibility, and disability information collected to consider or provide accommodations to students during training.

d. Course and training data, such as nomination forms, instructor lists, examination and course completion status, professional development, worksheets, training waivers, student identification number, course descriptions and schedules, enrollment and participation information, graduation dates, examination and testing materials, grades and student evaluations, aptitudes and personal qualities, course and instructor critiques, date graduated or eliminated with reasons for elimination, and information pertaining to training trends, needs, and assessments.

e. Equipment issued to trainees and other training participants, and other reports pertaining to training, such as credit hours accumulated, assignment history, curricula, and individual goals.

f. Professional development information, to include, mentor agreements, evaluations and performance documentations, career development planning, background and biographical information, civilian and military education information, and certifications.

g. Educational information, such as degree, major/minor, grade point average, institution name, academic status, and transcripts.

h. Financial information, such as payment records, and travel and other expenditures related to the training.

NOTE: Records pertaining to diploma and degree-conferring institutions, such as the military academies (United States Military Academy, United States Naval Academy, United States Air Force Academy, United States Marine Academy); the DoD Education Activity Schools, Uniformed Service University of the Health Sciences, and the National Defense University, are not part of this system of records

RECORD SOURCE CATEGORIES:

a. Individuals applying for or undergoing training, mentors, supervisors, instructors, and facilitators.

b. Academic institutions and/or other organizations supporting the development or delivery of DoD training, including training offered to select DoD personnel by the Intelligence Community.

c. All DoD databases flowing into or accessed through the following integrated data systems, environments, applications, and tools: the Defense Civilian Human Resources Management System (DCHRMS), Military Personnel (MILPERS), Department of Defense Voluntary Education System (DODVES), Defense Enrollment Eligibility Reporting System (DEERS), Army Training Requirement and Resources System (ATRRS), Total Workforce Management System (TWMS), Career Acquisition Personnel & Position Management Information System (CAPPMIS), Defense Civilian Personnel Data System (DPCPDS), Acquisition Career Management System (ACMS), Joint Personnel Adjudication System (JPAS), Medical Protection System (MEDPROS), and Management Information System (MIS II).

Figure E-3. Defense Training Records SORN, DoD 0005 – Page 3 of 7

d. Other DoD learning management systems, the data from which data is migrated into the DoD Enterprise Learning Modernization System.

e. Other federal government learning and student management systems, such as the Department of Education Postsecondary Education Participants System (PEPS), and State Departments of Education and their grant recipients.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

b. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

c. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

d. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

e. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

f. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

g. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Figure E-4. Defense Training Records SORN, DoD 0005 – Page 4 of 7

h. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

i. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

j. To the Office of Personnel Management to satisfy requirements to submit civilian employee training data in accordance with 5 CFR part 410.

k. To a Federal, State, tribal, local or foreign government agency or professional licensing authority in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance or status of a license, grant, or other benefit by the requesting entity, to the extent that the information is relevant and necessary to the requesting entity's decision on the matter.

l. To educational institutions or training facilities for purposes of enrollment and verification of employee attendance and performance.

m. To the Equal Employment Opportunity Commission, Merit Systems Protection Board, Office of the Special Counsel, Federal Labor Relations Authority, or Office of Personnel Management or to arbitrators and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties.

n. To the Department of Justice or a consumer reporting agency for further action on a delinquent debt when circumstances warrant.

o. To employers to the extent necessary to obtain information pertinent to the individual's fitness and qualifications for training and to provide training status.

p. To the United States Coast Guard Voluntary Education Program Office for the purpose of education counseling, financial management, and funds disbursement.

q. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

Figure E-5. Defense Training Records SORN, DoD 0005 – Page 5 of 7

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, agency, birth date, SSN, DoD ID number, or other DoD assigned student or educational ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

a. Non-mission employee training program records are maintained and disposed in accordance with National Archives and Records Administration General Records Schedule 2.6.

b. Mission-related training records are maintained and disposed in accordance with National Archives and Records Administration Schedules. The Military Departments, Joint Chiefs of Staff and OSD all retain in accordance with their individual Records and Information Management retention schedules.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD components safeguard records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including CAC authentication and password; SIPR token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the DoD office with oversight of the records. The public may identify the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, identifier (i.e., DoD ID Number or Defense Benefits Number), date of birth, current address, and telephone number of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

Figure E-6. Defense Training Records SORN, DoD 0005 – Page 6 of 7

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the appropriate system managers(s). Signed written requests should contain the full name, identifier (i.e., DoD ID Number or DoD Benefits Number), date of birth, and current address and telephone number of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3) and (d) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(6). In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), and (c), and published in 32 CFR part 310.

HISTORY: None.

Figure E-7. Defense Training Records SORN, DoD 0005 – Page 7 of 7

References

Children's Online Privacy Protection Act of 1998, 15 U.S.C. Chapter 91, §6501 - §6508.

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §1232g; 34 CFR Part 99.

FindLaw, State Legal Ages Laws, accessed March 2021, https://statelaws.findlaw.com/family-laws/legal-ages.html.

Grootens-Wiegers, Petronella et al, "*Medical decision-making in children and adolescents: developmental and neuroscientific aspects*," BMC Pediatrics, 2017, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5422908/.

Henning, Kristen, "*The Fourth Amendment Rights of Children at Home: When Parental Authority Goes Too Far*," Georgetown University Law Center, 2011.

Parent Coalition for Student Privacy, "*Legislative History of Major FERPA Provisions*," June 2002.

Parent Coalition for Student Privacy, "*Federal Laws Enabling Parents to Protect Their Children's Privacy: FERPA, PPRA and COPPA*," accessed March 2021, https://studentprivacymatters.org/ferpa_ppra_coppa/#COPPA.

Privacy Act of 1974, 5 U.S.C. § 552a.

Protection of Pupil Rights Amendment of 1978, 20 U.S.C. §1232h; 34 CFR Part 98.

Pub. L. 116-283, *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, January 1, 2021, p. 1875.

Pub. L. 116-92, *National Defense Authorization Act for Fiscal Year 2020*, December 20, 2019.

Pub. L. 107-107, *National Defense Authorization Act for Fiscal Year 2002*, December 28, 2001.

The Judge Advocate General's School, U.S. Army, JA 235, Government Information Practices — Casebook, Appendix A, March 2000.

U.S. Department of Defense 5400.11–R, "*Department of Defense Privacy Program*," May 14, 2007.

U.S. Department of Defense, Defense Privacy, Civil Liberties, and Transparency Division, Defense Training Records, DoD 0005, December 28, 2020.

U.S. Department of Defense Instruction 5400.11, "*DoD Privacy and Civil Liberties Programs*," January 29, 2019.

U.S. Department of Education, "*Privacy and Data Sharing*", accessed March 2021, https://studentprivacy.ed.gov/privacy-and-data-sharing.

U.S. Department of Education, Privacy Technical Assistance Center, "*FERPA Exceptions* Summary," PTAC – Handout – 2H, April 2014.

U.S. Department of Education, Student Privacy Policy Office, Protection of Pupil Rights Amendment (PPRA), SPPO–21–01, November 24, 2020.State Legal Ages Laws,"

Acronyms and Abbreviations

CETAP	Cybersecurity Education and Training Assistance Program (of the Department of Homeland Security)
CIO	Chief Information Officer (of the Department of Defense)
COPPA	Children's Online Privacy Protection Act
DA&M	Director, Administration and Management (of the Department of Defense)
DO&C	Directorate for Oversight and Compliance (of the Department of Defense)
DoD	Department of Defense
DoEd	Department of Education
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division (of the Department of Defense)
FERPA	Family Educational Rights and Privacy Act
FTC	Federal Trade Commission
FY	Fiscal Year
HASC	House Armed Services Committee
IDA	Institute for Defense Analyses
LEA	local educational agencies
NDAA	National Defense Authorization Act
NSA	National Security Agency
OMB	Office of Management and Budget
PAS	Privacy Act Statement
PEPS	Postsecondary Education Participants System (of the Department of Education)
PII	Personally Identifiable Information
PPRA	Protection of Pupil Rights Amendment
PTAC	Privacy Technical Assistance Center (of the Department of Education)
SEA	state educational agencies
SOR	System of Records
SORN	System of Records Notice
SSN	Social Security Number
STEM	science, technology, engineering, and mathematics
U.S.C.	United States Code
USD R&E	Under Secretary of Defense for Research and Engineering
USD P&R	Under Secretary of Defense for Personnel and Readiness

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-21	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Overview of Laws Governing the Potential Tracking of Students across DoD-Funded Science, Technology, Engineering, and Mathematics (STEM) Outreach Programs	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Stephen M. Olechnowicz, Michael S. Nash, W. Thomas Strickland, Ransee Peshala Wimalasena	BC-5-330912
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	D-21630

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Patrick Johnson, Chief, Workforce Management Directorate, and Chief, Cyber Excepted Service Branch Cyber Workforce Management Director, DoD Chief Information Officer 4800 Mark Center Drive, Alexandria, VA 22350-1800	DoD CIO
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Stephen M. Olechnowicz

14. ABSTRACT

Subsection (c) of Section 1726 of the National Defense Authorization Act for Fiscal Year 2021 (NDAA FY2021) directs the Secretary of Defense to submit to the Congressional defense committees a report on how Department of Defense (DoD) programs to train K-12 and postsecondary students in fields related to cybersecurity, cyber defense, and cyber operations can be better aligned and harmonized. One requirement of the report is to provide recommendations for mechanisms to track student participation and transition of student participation from one such program to another. During Department-wide discussions regarding this requirement, a principle DoD stakeholder organization raised concerns about the legality of tracking students who are minors. After an analysis of pertinent laws and a discussion with a senior privacy official from the DoD's Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD), the Institute for Defense Analyses (IDA) team assessed that it is permissible to use the Personally Identifiable Information (PII) of minors for the tracking purposes described in Section 1726, as long as DoD organizations comply with the Federal laws and DoD policies delineated in this document.

15. SUBJECT TERMS

NDAA FY 2021, privacy rights, minors, PII, Privacy Act, FERPA, K-12 students, tracking mechanisms

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			Unlimited	52	Patrick Johnson, Chief, Workforce Management Directorate, and Chief, Cyber Excepted Service Branch
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclassified	Unclassified	Unclassified			571-372-4592