PS4TLA: Privacy Support for the Total Learning Architecture

Specification Document, Volume 5: Policy Requirements

30 December 2019

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-12-2019	Research Report	January 2019 - December 2019

4. TITLE AND SUBTITLE
PS4TLA: Privacy Support for the Total Learning Architecture Volume 5 - Policy Requirements

5a. CONTRACT NUMBER
W911QY-16-C-0105-P00003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0603769D8Z

6. AUTHOR(S)
Dr. Bart P. Knijnenburg, Reza Ghaiumy Anaraky, Paritosh Bahirat, Yang He, Moses Namara, Dr. Erin Ash

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
CLEMSON UNIVERSITY
CLEMSON UNIVERSITY
OFFICE FOR SPONSORED PROGRAMS
1 CLEMSON UNIVERSITY

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
OUSD Personnel & Readiness
Advanced Distributed Learning Initiative
13501 Ingenuity Drive, Suite 248
Orlando, Florida 32826

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD/P&R/FE&T/ADLI

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this document is to outline how privacy regulations and recommendations outlined in Federal laws and memorandums, DoD Directives and Instructions, and standardized guidelines are applicable to Total Learning Architecture (TLA)-based systems. The set of recommendations put forth in this document will allow ADL and other TLA performers to build the TLA specifications and TLA-based systems with compliance to these regulations and recommendations in mind.
This document makes recommendations regarding the following aspects:
• The scope of privacy and the protection of PII as it is legally defined in light of DoD Components like the TLA infrastructure and its learning activities.
• Recommendations for safeguarding data using physical, technical, and managerial mechanisms.
• Guidelines for onboarding learning activities to make them a trusted and authenticated part of the TLA

15. SUBJECT TERMS
Privacy, Security, TLA, Total Learning Architecture, ADL, ADL Initiative, Advanced Distributed Learning, PII, Personally Identifiable Information, DoD Policy, DoDD, DoD Directives, DoDI, DoD Instructions, standards, specifications, Learning Ecosystem, Safeguarding Data, Procedures, Sensitivity Levels, Disclosures, Consent, Notifications, Federal Register, Privacy Act,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Nick Armendariz
U	U	U	UU	23	19b. TELEPHONE NUMBER *(Include area code)* 407-381-5550

PS4TLA: Privacy Support for the Total Learning Architecture

Specification Document, Volume 5:

Policy Requirements

Author information

Project lead: Dr. Bart P. Knijnenburg, Clemson University
Project team: Reza Ghaiumy Anaraky, Paritosh Bahirat, Yang He, Moses Namara, Dr. Erin Ash
Technical point of contact: Andy Johnson, Advanced Distributed Learning (ADL) Initiative

Recommended citation: Knijnenburg, B.P., Ghaiumy Anaraky, R., Bahirat, P, He, Y., Namara, M., Ash, E., and Johnson, A. (2018) "Privacy Support for the Total Learning Architecture: Policy Requirements". PS4TLA Specification Document, v5, Clemson University, Clemson, SC. Available at: http://www.usabart.nl/PS4TLA/spec5.pdf.

Executive summary

The purpose of this document is to outline how privacy regulations and recommendations outlined in Federal laws and memorandums, DoD Directives and Instructions, and standardized guidelines are applicable to Total Learning Architecture (TLA)-based systems. The set of recommendations put forth in this document will allow ADL and other TLA performers to build the TLA specifications and TLA-based systems with compliance to these regulations and recommendations in mind.

This document makes recommendations regarding the following aspects:

- The **scope of privacy** and the protection of PII as it is legally defined in light of DoD Components like the TLA infrastructure and its learning activities.
- Recommendations for **safeguarding data** using physical, technical, and managerial mechanisms.
- Guidelines for **onboarding learning activities** to make them a trusted and authenticated part of the TLA ecosystem, which includes cybersecurity training, a Privacy Impact Assessment, and a publication of the learning activity in the federal register.
- Procedures to follow when requesting (learning activities) and providing (TLA infrastructure) **access to personal information**, including notice, consent, and disclosure accounting.
- Guidelines regarding **data, devices, and authentication**, to regulate who can access what information from which devices.
- Procedures to follow in case of **violations and review** requirements to prevent such violations.

It is important to note that this document provides a **non-exhaustive** analysis of the most prominent laws, directives, and guidelines. The authors of this document do not guarantee that following the recommendations described herein ascertain compliance with all rules that predate it. Moreover, the document provides no comparison against directives and guidelines in other sectors to fill potential gaps in the policy landscape as it pertains to TLA.

Scope of privacy

It is DoD policy that an individual's privacy is a fundamental legal right that must be respected and protected (DoDD 5400.11, paragraph 3.a). This, translates to a series of privacy requirements regarding the collection, storage and use of Personally Identifiable Information (PII). The privacy requirements outlined in the DoD Privacy Program (DoD 5400.11-R) differ for "DoD Components" and "third parties". Moreover, rules regarding "disclosure within the DoD" are different from rules regarding disclosures to and from third parties. This section defines the concept of PII and establishes which set of rules applies to the TLA infrastructure and the learning activities that connect to the TLA.

Personally Identifiable Information (PII)

PII is any information about an individual maintained by an agency

According to the US Government Accountability Office (GAO report 08-536), "PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, and (2) any other information that is linked or linkable to an individual information." The report notes that this is an amalgam of the definitions put forward in OMB M-07-16 and OMB M-06-19.

Citing this definition, the NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) gives the following examples of PII (NIST SP 800-122, section 2.2):

- Name: such as full name, maiden name, mother's maiden name or alias.
- Personal Identification Number: such as social security number (SSN; the use of social security numbers within DoD forms should be reduced or eliminated whenever possible in accordance with DoDI 1000.30), passport number, driver's license number, taxpayer identification number, or financial account or credit card number.
- Address Information: such as street or email address.
- Personal characteristics: including photographic images especially of the face, fingerprints, handwriting, or biometric data (e.g., retina scan, voice signature, facial geometry, see DoDD 8521.01E).
- Other information about an individual that is linked or linkable to one of the above: such as date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information.

Assumption: Based on ample real-world and scientific evidence (see PS4TLA Spec 4, "levels of identifiability"), advances in the field of "re-identification" show that the category of "other information" expressed above may cover any and all information that pertains to an individual, as it has been shown that, when used in aggregate, almost all information can enhance the linkability of a dataset to the other categories of PII. Indeed, OMB M-10-22 states that "non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual." NIST SP 800-122, Section 2.1 refers to such information as Linked Information.

Suggestion: To be on the safe side, TLA-based systems should assume that all collected data constitutes PII, and hence they are subject to the privacy protections outlined in this document.

The TLA infrastructure

The TLA infrastructure is considered a system of records

The Total Learning Architecture (TLA) is a set of specifications to enable the development of next generation learning systems. In managing learners' learning activities and learning outcomes, TLA produces and processes records that identify users by their name, email address, and/or other personally identifiable information (PII). As such, any implementation of TLA can be considered a system of records, which is defined as "a system that retrieves records by name or PII that is under control of DoD." (DoD 5400.11-R, chapter 1).

Assumption: The learner record stores by TLA exist within a DoD security enclave. Hence, from the perspective of privacy, any use of this information by DoD entities is considered a "disclosure within the DoD" (DoD 5400.11-R, section 4.2.1).

Even if the certain learner data is stored outside the DoD security enclave, it is the responsibility of the TLA to "Ensure that safeguards for protected information stored at secondary sites are appropriate." (DoD 5400.11-R, section AP1.3.5)

Learning activities

Virtually all learning activities process PII

DoD 5400.11-R, section AP1.1.2 suggests that "PII must also be protected while it is being processed or accessed in computer environments outside the data processing installation." This applies to activity providers that connect to TLA and process PII, even if they are considered to exist outside the data processing installation of the TLA environment.

Activity providers could potentially avoid handling PII, by using the TLA as an identification gateway: in this setup, the TLA system would authenticate learners, which would then interact with learning activities in a pseudonymous or anonymous manner (NIST SP 800-122, section 4.2). Completely anonymous interactions are unlikely to be the norm, though, as they would have to be completely stateless. This would prevent the learning applications from conducting any type of personalization across multiple user sessions (PS4TLA Spec 4, "levels of identifiability"). Moreover, as mentioned above, pseudonymous users can be re-identified through cross-referencing the de-identified data with other datasets, which means that even the data that is collected pseudonymously should conservatively be classified as PII.

Suggestion: To be on the safe side, TLA-based systems should assume that all learning activities process PII, and hence they are subject to the privacy protection responsibilities outlined in this document.

Contracted and enclaved learning activities are under control of DoD

Learning activities that are developed and maintained as a DoD Component contract are considered to be maintained by the DoD Component" (DoD 5400.11-R, section 1.3.1) and are thus considered a system of records. As such, they are considered a DoD entity, and disclosure to the learning activity is considered a "disclosure within the DoD" (DoD 5400.11-R, section 1.3.4). The same is true for disclosure from the learning activity to other systems of records (including the TLA infrastructure) (DoD 5400.11-R, section 4.1.2).

Assumption: This is also true for any learning activity that operates within a DoD security enclave (even if it is not a contracted component).

System of records rules may not apply to learning activities that are open to non-DoD students

System of records rules do not apply to records that are "maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and commingled with training records of other students (for example, admission forms, transcripts, academic counseling and similar records)" (DoD 5400.11-R, section 1.3.1.3.3). This suggests that learning activities that are open to non-DoD students (and that do not store DoD-student data in a separate repository) fall outside the system or records regulations (i.e., the "third parties" rules apply; see below).

All other learning activities are considered "third parties"

All other non-DoD entities are considered to be "third parties"; but even they can process PII with the TLA infrastructure, under provisions stipulated in DoD 5400.11-R, chapter 4. DODI 8550.01, enclosure 3, paragraph 3.c advises that links to third-party systems should be clearly disclaimed.

Suggestion: Develop TLA system capabilities (e.g. an API) that can manage the processing of PII in accordance to regulations for both "disclosure within the DoD" as well as disclosures to and from "third parties".

Safeguarding data

The DoD Privacy Program (DoDD 5400.11) outlines a number of general responsibilities, minimum standards, and guidelines for IT safeguards that apply to DoD Components. This section describes these rules in the context of the TLA infrastructure and the learning activities.

General responsibilities and minimum standards

The TLA infrastructure and learning activities must protect records against privacy threats

DoD 5400.11-R, section 1.4.1 states that "DoD Components shall establish appropriate administrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept."

More specifically, DoD 5400.11-R, sections 1.4.2 and AP1.1.3 state that:

- Classified material is protected by virtue of the fact that IT facilities authorized to process it already have adequate procedures and security in place (DoD 5400.11-R, section AP1.1.3). Classified material should be labeled as such (DoD 5400.11-R, section AP1.3.3).
- DoD 5400.11-R, section 1.4.2: Personal information that would normally be withheld from the public (as outlined in FOIA exemption 6, i.e., personnel and medical data that would constitute an invasion of privacy) must be treated in accordance to the DoD Information Security Program (DoD 5200.1-R).
- All other data must be protected commensurate with the nature, type, and sensitivity of information involved; the risk of exposure; and the vulnerabilities of the system (DoD 5400.11-R, sections 1.4.2 and AP1.3.1).
- The latter two types of data must be accessed and processed following "FOUO" procedures (DoD 5400.11-R, section AP1.1.3), and should be marked as such (DoD 5400.11-R, sections AP1.3.2 and AP1.3.4).

Suggestion: As mentioned above, it is best to treat all data collected by TLA-based systems as if it were PII. Hence, all data should be treated in accordance to the DoD Information Security Program and following "FOUO" procedures.

IT Safeguards

DoD 5400.11-R: Appendix 1 states that "special considerations must be given to safeguarding personal information in IT systems consistent with the requirements of DoD Directive 8500.1." It further outlines a number of guidelines for physical, technical, and procedural safeguards. In establishing safeguards, the sensitivity of the data, the installation environment, the risk of exposure, and the cost of the safeguard must be considered (DoD 5400.11-R, section AP1.3.1).

Physical safeguards must be in place to prevent unauthorized access to devices that store, access, and/or process TLA data

Guidelines for physical safeguards include:

- Access procedures for unclassified areas that process or contain PII (DoD 5400.11-R, section AP1.4.2).
- Protection of on-line devices that contain or process information from systems of records (DoD 5400.11-R, section AP1.4.3).
- Proper disposal of paper records (DoD 5400.11-R, section AP1.4.4).

Technical safeguards prevent unauthorized access to TLA data

Guidelines for technical safeguards include:

- Treat PII not cleared for release as "sensitive" (DoDI 8500.2 and DoD 5400.11-R, section AP1.5.1).
- Encrypt PII in accordance with Information Assurance (IA) policies and procedures (DoDI 8500.2 and DoD 5400.11-R, section AP1.5.2).
- Remove personal data from drives in a manner that precludes reconstruction (DoD 5400.11-R, sections AP1.5.3, AP1.7.1 and 1.4.3).
- For remote access, use only DoD authorized devices (DoD 5400.11-R, section AP1.5.5) and follow IA policies and procedures (DoD 5400.11-R, section AP1.5.6).
- Minimize access to data fields necessary to accomplish an employee's task (DoD 5400.11-R, section AP1.5.7).
- Do not totally rely on proprietary software for data protection (DoD 5400.11-R, section AP1.5.8).
- Reduce PII holdings to the minimum necessary for proper of DoD's functions (OMB M-07-16 and NIST SP 800-122, section 4).

Suggestion: PS4TLA Spec 4 ("Collection of various data types") suggests "a combination of strict access control, encryption, de-identification and obfuscation" to protect learner runtime data against PII leakage and inference attacks. These suggestions are in line with the stipulated requirements. Beyond this, TLA must regulate physical access to TLA systems, proper erasure/disposal of data, and the use of authorized devices.

Special procedures must be followed by TLA system managers and activity providers

Special procedures for managers include:

- Preparing and submitting system notices, amendments and alterations (DoD 5400.11-R, section AP1.6.1.1). This is covered in "publishing to the federal register" below.
- Maintaining access authorizations for individuals (DoD 5400.11-R, section AP1.6.1.2).
- Regularly reviewing holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting DoD's purposes and mission. This may require the development of a schedule for periodic review of PII holdings (OMB M-07-16 and NIST SP 800-122, section 4).
- Preparing Privacy Impact Assessments (PIAs) consistent with USC title 44, section 3501 (DoD 5400.11-R, section AP1.6.1.3). This is covered in "Privacy Impact Assessment" below.
- Privacy Act training of personnel requiring access to the data (DoD 5400.11-R, section AP1.6.1.4). This is covered in "Training requirements" below.

Suggestion: Provide TLA system managers with a tool to manage access authorizations (other aspects are covered below).

Onboarding learning activities

This section describes a number of privacy requirements that must be met for a learning activity to become part of a TLA-based environment. This section describes the training, Privacy Impact Assessment and publication in the Federal Register that must be completed as part of these onboarding activities.

Training requirements

Everyone involved with TLA must complete a Privacy Act orientation training

DoD 5400.11-R, section 7.1 states that "The Privacy Act (USC title 5, section 552a) requires each Agency to establish rules of conduct for all persons involved in the design, development, operation, and maintenance of any system of record and to train these persons with respect to these rules." Assigning such training is the responsibility of the system manager (DoD 5400.11-R, section AP1.3.7).

As a prerequisite, each individual must complete a periodic (DoD 5400.11-R, section 7.4.3) orientation that "provides basic understanding of this Regulation (DoD 5400.11-R) as it applies to the individual's job performance." (DoD 5400.11-R, section 7.3.2.1).

Suggestion: Since all TLA users (even end-users) deal with PII (if anything, their own), the orientation should be assigned to all TLA users. Web-based training is the most appropriate format for this (DoD 5400.11-R, section 7.4.4). Training should follow guidelines outlined in NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program." Security education should be a continuous, rather than a periodic influence on individual security performance. As a minimum, this involves an annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training (DoD 5200.1-R, section 9.4).

Specialized training is required for developers, operators, statisticians, and managers

Specialized training should be given to, e.g., system developers, system operators, statisticians (DoD 5400.11-R, section 7.3.2.2) and managers (DoD 5400.11-R, section 7.3.2.3). Since this includes system developers, this requirement also applies to the personnel of activity providers involved in developing learning activities.

Assumption: Most system developers have already completed such training, as part of the FedRAMP program. Likewise, most operators, statisticians and managers have already completed security training, as outlined by the DoD Information Security Program (DoD 5200.1-R, chapter 9).

Suggestion: Develop a training for the developers of learning activities, which covers relevant parts of this document as well as certain privacy considerations outlined in PS4TLA Spec 4. Materials may also include external resources such as those developed by the DoD Security Institute. Relevant personnel of activity providers must complete this training to get up to speed about the privacy considerations surrounding the TLA. Training for personnel who are cleared for access to classified information must include the following topics: roles and responsibilities, classifying and declassifying information, and safeguarding (DoD 5200.1-R, section 2.1.1). Security education should be a continuous, rather than a periodic influence on individual security performance. As a minimum, this involves an annual refresher training that reinforces the policies, principles and procedures covered in initial and specialized training (DoD 5200.1-R, section 9.4).

Privacy Evaluation and Impact Assessment

System managers must conduct a privacy evaluation

The manager of a system of records is required to "evaluate the information to be included in each new system before establishing the system" (DoD 5400.11-R, sections 1.1.6.1 and AP1.6.1.3). This evaluation is also required for alterations or amendments to existing systems (DoD 5400.11-R, section 1.1.6.1),

In conducting their evaluation, managers must consider the following (DoD 5400.11-R, section 1.1.6.2):

- The relationship between each collected item information and its purpose.
- The necessity and relevancy of the information to the purpose of collection (DoDI 8910.01 and DoDI 7750.07 require that collected information is essential to the mission of the requesting organization and the cost of the collection is worth the benefit derived from it).
- Impact of not collecting the information on the purpose or mission of the system.
- The possibility of not using PII.
- The length of time each item needs to be retained.
- The cost of maintaining the information.

Suggestion: Each learning application must include a reference to this evaluation in its request to be included in a TLA-based system.

System managers must conduct a Privacy Impact Assessment (PIA)

The aforementioned evaluation overlaps considerably with a Privacy Impact Assessment (PIA), which Federal agencies are required to conduct per the E-Government Act of 2002 (Public Law 107–347). Procedures for DoD regarding PIA are outlined in DoDI 5400.16 and Public Law 107–347, section 208.b. According to these regulations (DoDI 5400.16, section 1a), review is required for:

- New systems *before* they are developed, purchased, or contracted.
- The conversion of paper-based records to electronic systems.
- The conversion of anonymous data to PII.
- Alterations to systems that create new privacy risks, such as: management changes, merging, new public access, inclusion of commercial sources of PII, new interagency uses, alteration of the character of the data.

According to Public Law 107–347, section 208.b, a PIA addresses:

- What information is to be collected.
- Why the information is being collected.
- The intended use of the information.
- With whom the information is shared.
- Procedures for notice and consent.
- How the information will be secured.
- Whether the system can be considered a “system of records”.

A PIA is prepared using DD Form 2930 and reviewed by:

- The component’s senior information security officer, for compliance with DoD cybersecurity polices.
- The component’s privacy officer, for compliance with DoD 5400.11-R.
- The component’s CIO, for final approval.

Section 1 of DD Form 2930 must be published publicly until PII is no longer maintained in the system or the system is no longer operational (DoDI 5400.16, section 3; Public Law 107–347, section 208.b).

Suggestion: Each learning application must include a public link to its DD Form 2930 in its request to be included in a TLA-based system.

Publication in the Federal Register

DoD 5400.11-R, section 6.1 states that systems of records must publish four types of documents relating to the Privacy Program in the Federal Register:

- Privacy procedural rules.
- Exemption rules.
- System notices.
- Match notices.

Learning activities must publish additional and/or exempted privacy rules to the Federal Register

By default, all procedural rules of the Privacy Program (DoD 5400.11-R) and the Privacy Act (USC title 5, section 552a) apply to a learning activity that is considered a system of records. However, if the learning activity wishes to establish additional privacy procedural rules and/or to be exempted from certain rules, those additional procedures and exemptions must be published in the Federal Register (DoD 5400.11-R, sections 6.1.4 and 6.1.5).

Suggestion: If the TLA requires learning activities to follow privacy requirements to extend beyond the ones outlined in the Privacy Program and the Privacy Act, it may require learning activities to publish these requirements in the Federal Register.

Exemptions must include the system identifier and name, the section of the Privacy Act that is exempted, the section of the Privacy Act that warrants the exemption, and the specific reasons why an exemption is being claimed (DoD 5400.11-R, section 6.2.2).

Blanket exemptions exist for classified material (DoD 5400.11-R, section 5.1.3), testing materials (if it would compromise the examination process), and evaluations for promotion (if it would compromise promised confidentiality).

Suggestion: TLA must be cognizant of these blanket exemptions by refraining from (inadvertently) disclosing testing materials and confidential evaluations.

A system notice must be published in the Federal Register for each learning activity

System notices are submitted to the Defense Privacy Officer (DPO) in Federal Register format. The DPO transmits them to the Federal Register for publication (DoD 5400.11-R, section 6.1.6.2). A system of records cannot be operated until its system notice is published (DoD 5400.11-R, section 6.1.6.1). A 40-day review period is required (DoD 5400.11-R, section 6.4.4).

A system notice contains the following components:

- The ID, name, and physical location of the system (DoD 5400.11-R, sections 6.3.2–4).
- The kinds of records that are stored (DoD 5400.11-R, section 6.3.6); this does not apply to source data that is used to generate a record and then destroyed.
- Source categories (i.e., where data was obtained) (DoD 5400.11-R, section 6.3.15).
- The intended users to which the data pertains (DoD 5400.11-R, section 6.3.5); this description should not be overgeneralized.
- Who ordered/mandated the existence of the system (DoD 5400.11-R, section 6.3.7).
- Who manages the system (DoD 5400.11-R, section 6.3.11).
- How users can access their own data and contest it if needed (see below) (DoD 5400.11-R, sections 6.3.12–14).
- The purpose of the system (i.e., its internal routine uses) (DoD 5400.11-R, section 6.3.8).
- The external routine uses (DoD 5400.11-R, section 6.3.9); the public must be given 30 days to comment on these proposed routine uses (DoD 5400.11-R, section 6.1.6.1.2). Note that some blanket routine uses exist, such as hiring, contracting, licensing, awarding grants, and determining salaries (DoD 5400.11-R, section AP3).
- Policies and practices for storing (the storage medium), retrieving (by which ID), accessing, safeguarding (the physical and procedural safeguards, but not the technical safeguards), retaining and disposing the data (DoD 5400.11-R, section 6.3.10).
- Exemptions claimed for the system (DoD 5400.11-R, section 6.3.16).

System notices must be resubmitted upon making significant alterations to the system of records (DoD 5400.11-R, section 6.4), e.g. when there are changes to the types intended users, the kinds of records stored, the manner of use, and/or the ease of accessing the data.

Suggestion: A system's data collection and use practices in the TLA environment can be authorized against its published system notice. Each learning application must include a link to its system notice in its request to be included in a TLA-based system.

> *A match notice may be required for the TLA infrastructure, but not for learning activities*

Match notices apply to the Computer Matching Program, which covers the cross-referencing of data against Federal personnel records (DoD 5400.11-R, chapter 11). In TLA such a match may be required to authenticate a user (e.g., to make sure that degrees or credentials are awarded to the correct person). Most likely this authentication happens in the TLA infrastructure and not in the underlying learning activities.

Suggestion: The TLA infrastructure should publish a match notice for the purpose of authenticating users.

> *While probably not required, Privacy Act statements for routine uses of the information may be published in the Federal Register*

Beyond the four documents mentioned in DoD 5400.11-R, section 6.1, systems of records that wish to disclose information to "third parties" must also publish Privacy Act statements of all routine uses of this information in the Federal Register (DoD 5400.11-R, section 4.2.3.2.4).

Suggestion: Learning activities can avoid disclosure to third parties by using TLA as a knowledge broker: The learning activity discloses the information to the TLA infrastructure (internal use), and the TLA infrastructure discloses the information to third parties (as needed for their operation).

That said, Privacy Act statements are also needed to furnish notice and consent (see "Notifying the user" below). Hence it would be best for learning applications to publish such Privacy Act statements anyway. The contents of a Privacy Act statement are described below under "Notifying the user".

Suggestion: Since this statement must be made available anyway, learning activities should just publish it in the Federal Register.

Access to Personal Information

This section describes several requirements regarding the collection and use of personal information by systems of records. The two most important requirements in this regard are:

- Whenever possible "information should first be collected from the individual" rather than from other sources (DoD 5400.11-R, section 2.1.3).
- Disclosure is "mandatory only when the DoD Component is authorized to impose a penalty on the individual for failure to provide the requested information (DoD 5400.11-R, section 2.1.5).

Assumption: In most cases, neither the TLA infrastructure nor the activity providers are authorized to impose such a penalty, hence disclosures are considered voluntary by default.

> *Given that personal data disclosures are voluntary by default, TLA must furnish a notice and consent procedure*

While personal information should first be collected from the individual, TLA can furnish information in a learner record store to a learning activity upon the request of the individual (DoD 5400.11-R, section 2.1.3.4). In fact, furnishing already collected information is DoD policy: DoDI 8910.01 requires that information to be collected is not duplicative of information already available. This process of furnishing information to a learning activity would be subject to notice and consent, and the rules around these procedures are covered in this section.

Notifying the user

Notice must be provided via a Privacy Act statement

DoD 5400.11-R, section 2.1.4 states that a Privacy Act statement must be provided when personal information is requested. This statement is only required if the information will be added to a system of records (i.e., the collection of temporary information is not subject to this requirement).

According to DoD 5400.11-R, section 2.1.4.2, a Privacy Act statement must include:

- The executive order that authorizes the collection of the requested information.
- The purposes for which the information is to be used.
- The routine uses of the information.
- Whether providing the information is voluntary or mandatory.
- The effects on the individual if he or she chooses not to provide the requested information.

Suggestion: TLA can automatically generate Privacy Act statements from their Federal Register entries (given that they are all published there, as suggested above). A benefit of this approach is that it is aligned with guidance requiring government agencies to translate privacy policies into standardized machine-readable format (Public Law 107–347, section 208.c(2)).

Privacy Act statements must be conspicuously displayed and easy to understand

Privacy Act statements must be concise, current, and easily understood (DoD 5400.11-R, section 2.1.4.3). They must be conspicuously displayed (DoD 5400.11-R, section 2.1.4.4). The individual is not required to sign the statement (DoD 5400.11-R, section 2.1.4.5). While no standardized statement exists, one can refer to DoDI 8550.01, enclosure 3, paragraph 4.d for an example.

Suggestion: Research suggests that many users ignore privacy notices. PS4TLA Spec 4, "Privacy Notices" suggests giving users a quick overview of privacy practices using "nutrition labels", making notices "textured" as a means to provide access to more detailed information, and using comics to make notices more approachable. Moreover, User-Tailored Privacy (PS4TLA Spec 4, "Adapt the justification") may be used to adaptively highlight aspects of the Privacy Act statement that are particularly relevant to this specific user and their situation.

Suggestion: An information collection control symbol should be part of the Privacy Act statement. DoDI 8910.01 requires that information collected must be approved and assigned a Component information collection control symbol. If information is collected across components, it must be approved and licensed with a DoD internal information collection report control symbol (RCS).

Suggestion: In line with DoDI 8550.01, enclosure 3, paragraph 1.i, display the Privacy Act statement in close proximity to the actual information request: either on the same page, or on an interstitial page right before the requesting page (PS4TLA Spec 4, "Adapt the justification"). Ask users to acknowledge the statement with a mouse click.

Obtaining consent

Consent is required whenever personal data is collected from third parties (DoD 5400.11-R, section 2.1.3) or disclosed to third parties (DoD 5400.11-R, section 4.1).

In-the-moment consent is not required for routine uses that match the purpose for which the data is being maintained

According to DoD 5400.11-R, section 4.2.1, consent is not needed for internal disclosure if the requester needs it to perform his or her assigned duties and the intended use relates to the purpose for which the record is maintained. This provision only gives access to the minimally required records.

Moreover, according to DoD 5400.11-R, section 4.2.3, consent is not needed for **external** disclosure if is part of routine use, which means that it must:

- Be compatible with the purpose for which the record was collected, identify the person or organization to whom record may be released.
- Identity of person or organization to whom the record may be released.
- Identify the specific uses of the record.
- Be published in federal register as a routine use.

Suggestion: TLA can forego requesting consent if the person or application requesting the information is authorized to use the information (which can be checked against the access authorization database or the Federal Register) and if the stated purpose and routine use are mentioned in the published system notice of the system of records that maintains the information.

Suggestion: For all other requests, the TLA-based system should ask the user for explicit consent. This consent should be documented, so that it does not have to be requested again when the same situation (same recipient, same information, same purpose) occurs.

Consent for routine uses should be requested with the delivery of the Privacy Act statement

Consent is still required for routine uses, because most disclosures are considered voluntary. For these cases, it makes more sense to request consent once, when delivering the Privacy Act statement.

Suggestion: Request consent as part of the delivery of the Privacy Act statement. Specifically, within the Privacy Act statement, itemize the routine uses of each type of information, ask the user to provide explicit consent to the collection and each routine use of the information.

Suggestion: In line with PS4TLA Spec 4 ("Adapt the setting"), the TLA may employ User-Tailored Privacy to provide adaptive default settings for these consent requests.

Disclosure accounting

DoD components must keep a record of all disclosures made

DoD 5400.11-R, section 4.5 states that DoD components must "keep an accurate record of all disclosures made from any system of records", unless it is to personnel for use in the performance of their official duties or required by USC title 5, section 552a.

Disclosure accounts must contain the date, description of information, purpose, and the name and address of the person or Agency to whom the disclosure was made (DoD 5400.11-R, section 4.5.2). Records must be maintained for 5 years after disclosure or the life of the record, whichever is longer (DoD 5400.11-R, section 4.5.5).

Suggestion: TLA-based systems must keep a database of all disclosures made.

Individuals must be given access to disclosure accountings

DoD components must make all disclosure accountings available to the individual to whom the record pertains, except when the system of records has been exempted from this requirement (DoD 5400.11-R, section 4.5.6).

Suggestion: TLA-based systems can implement a "disclosure accountings viewer" as part of the "data scrutability tool" proposed below (see "Individual access").

Individual access

Users must be given access to the information collected about them

DoD 5400.11-R, section 3.1 states that information collected by a system of records must be made available to the individual to whom the information pertains. Requests for access to personal information should be addressed to a system manager or designated office (DoD 5400.11-R, section 3.1.2). Users may be required to provide proof of identity, but this procedure must not be overly complicated (DoD 5400.11-R, section 3.1.3).

Assumption: Authentication as a logged-in TLA user is sufficient proof of identity for the purpose of this request.

Users who request access to their information must be given an exact copy of the record without any changes or deletions (DoD 5400.11-R, section 3.1.4), unless exemptions are claimed as described in the Federal Register (DoD 5400.11-R, section 5; and USC title 5, section 552a).

Access request can be denied based on exemptions, and are subject to an appeal process

Access requests can be denied if the record is classified or exempted, or if the individual is not authorized to access the system containing the record (DoD 5400.11-R, section 3.2.1). Denials must be in writing and include the denial authority, date of denial, reason for denial, and a notice of the right to appeal within 60 days (DoD 5400.11-R, section 3.2.3).

Appeals must be reviewed within 30 days by the component head or a designee. If the appeal is denied, written notification must include the appeal authority, date of determination, reason for the denial, and a notice of the right to seek judicial relief (DoD 5400.11-R, section 3.2.4).

Users must be allowed (and should be encouraged) to review the information about themselves and request changes when errors are found

DoD 5400.11-R, section 3.3 states that "individuals are encouraged to periodically review the personal information being maintained about them by the DoD Components and to avail themselves of the procedures established by this Regulation and other Regulations to update their records."

Amendment requests are limited to factual information; judgments such as performance ratings or promotion appraisals are not subject to amendment (DoD 5400.11-R, section 3.3.2.1). Amendment requests must include a description of the item or items to be amended, reason for amendment, the type of action sought (deletion, correction, addition), and available evidence supporting the request (DoD 5400.11-R, section 3.3.2.3). The burden of proof is on the individual ((DoD 5400.11-R, section 3.3.3). According to the Privacy Act (USC title 5, section 552a) amendments must be processed within 10 business days.

Users may be required to provide proof of identity, but this procedure must not be overly complicated (DoD 5400.11-R, section 3.3.4).

Assumption: Authentication as a logged-in TLA user is sufficient proof of identity for the purpose of this request.

If the request for amendment is granted, the record must be amended accordingly and the requester must be notified of this change (DoD 5400.11-R, section 3.3.8). Moreover, "all DoD Components and Federal Agencies known to be retaining the record or information […] shall be notified of the amendment" (DoD 5400.11-R, section 3.3.9). The requester must be advised of these notifications. The disclosure accounting records can be used to keep track of these previous disclosures.

Suggestion: The TLA infrastructure should contain a mechanism that allows amendments to a record to be automatically federated to previous recipients of the record.

Amendment request can be denied based on exemptions, and are subject to an appeal process

If the request for amendment is denied in whole or in part, the individual must be advised in writing of this decision (DoD 5400.11-R, section 3.3.10). The denial must include the specific reason and authority for not amending, a notification that he or she may seek further independent review, and procedures and reference to assistance for appealing the decision.

Appeals must be processed within 30 days, unless the appeal authority determines that more time is needed. If the appeal is denied in whole or in part, the individual must be notified in writing by the reviewing official (DoD 5400.11-R, section 3.3.11). The denial must contain the specific reason and authority for the denial, a notification that a statement of disagreement may be filed, and a notification that the individual may seek judicial review of the decision.

If properly filed, a statement of disagreement must be included in the records and furnished to all future and prior recipients of the disputed records (DoD 5400.11-R, section 3.3.11.2.3).

Suggestion: The TLA learner record stores should have the ability to annotate any record with a statement of disagreement, that would then automatically be disclosed alongside any disclosure of the record itself.

Inspection and amendment can be automated by implementing a "data scrutability tool"

The manual inspection and amendment processes seem inadequate in light of the digital data collection facilities of the TLA. It should be possible to provide TLA users automated access to their personal records, amendment opportunities, and disclosure accountings (see "Disclosure accounting"). This process can be further streamlined by pre-designating certain information as exempt from inspection and/or amendment, so that only eligible information and amendment opportunities are provided to the user.

Assumption: System managers are allowed to pre-authorize the release of recorded information about a user to the user themselves for inspection and/or amendment.

Suggestion: TLA-based systems should contain a "data scrutability tool" (PS4TLA Spec 4, "Scrutability and the quantified self") that automates the inspection and amendment facilities required by DoD 5400.11-R, section 3. This tool should contain all information collected about the user (excluding confidential or exempted information), with for each piece of information a link to an amendment request form (excluding judgments or exempted information) and an account of past disclosures (excluding confidential or exempted disclosures).

Public access to information

DoD may determine that certain information collected or generated by TLA-based systems should be disseminated to a broader audience. This can be done, provided that is done in a manner that protects privacy (Public Law 107–347, section 204.a), through a DoD Internet Service or Internet-based Capability (IbC), which is governed by DoDI 8550.01.

TLA-based data can be disseminated via a public or private DoD Internet Service / IbC if there is a need and if the data can be declassified or redacted

The appendix to DoDI 8550.01, enclosure 3 outlines the information review process that must be used to establish a DoD Internet Service or IbC. If DoD establishes a need to disseminate certain TLA-based data (e.g. public reports of trends in the learned capabilities of DoD personnel), it can decide to establish an Internet Service or IbC to disseminate this information. This is only possible for unclassified, declassified, or redacted data. Moreover, if the data is not intended or authorized for public release (e.g. FOUO), then the dissemination must happen through a private DoD Internet Service, subject to access controls.

Suggestion: Aggregate TLA-based data may be considered for dissemination via a public DoD Internet Service or IbC, subject to the requirements and guidelines outlined in DoDI 8550.01.

Suggestion: TLA-based data that is not sufficiently aggregated should be considered as PII, and its dissemination should therefore adhere to FOUO. If dissemination is needed, it must occur via a private, access-controlled DoD Internet Service, subject to the requirements and guidelines outlined in DoDI 8550.01.

Data, devices and authentication

Sensitivity levels of data

DoDI 8520.03, section 2c describes four levels of sensitivity for unclassified information. Sensitive information is automatically classified as Sensitivity Level 3, unless the information owner determines that the data meets the criteria for Levels 1, 2 or 4.

Most of the unclassified data in TLA can be considered Sensitivity Level 1

Data with Sensitivity Level 1 is "personal in nature, pertains to only a single individual, and would have a low adverse impact on the efficacy of DoD missions if the information were compromised (e.g., lost; misused; or accessed, modified, or distributed without authorization)" (DoDI 8520.03, section 2c.1). Training records are explicitly mentioned as an example of such data.

Suggestion: Designate TLA-based data as Sensitivity Level 1 by default and treat the data accordingly.

Learning materials can be considered Sensitivity Level 2

Data with Sensitivity Level 2 has been provided by a source "under the condition that it not be released to other parties and would have a low or moderate adverse impact on the efficacy of DoD missions or the reputation of the DoD if the information were compromised." Examples of this information include a company's proprietary information. In many cases, the learning materials contained in a learning activity fit this Sensitivity Level: learning materials are often proprietary, and in some cases an advance knowledge of the materials (e.g., the content of tests) would have an adverse impact on the mission of the system.

Suggestion: Designate learning materials as Sensitivity Level 2 by default and treat the data accordingly.

Accumulated TLA data can be considered Sensitivity Level 3

Data with Sensitivity Level 3 could "adversely affect DoD mission interests and would have a moderate or high impact on the efficacy of DoD missions if the information were compromised." As a whole, TLA can be considered a "personnel management system" which is explicitly mentioned as an example of data with Sensitivity Level 3. As such, one may argue that any sufficiently large subset of TLA data as to constitute "personnel management data" can be considered to be at Sensitivity Level 3.

Suggestion: Treat (access to) any sufficiently large subset of TLA-based data as Sensitivity Level 3.

Special consideration to Sensitivity Level 3 must be given to situations where TLA performs a "computer match" to e.g. authenticate users against federal personnel data. This can only be done if there is a Computer Matching Agreement (CMA) in place (DoD 5400.11-R, chapter 11), which must contain a purpose, legal authority, justification (why use computer matching?), record description (what, who, frequency), processes to ascertain and verify the accuracy of the information (including procedures for due process), requisite notices (Privacy Act statement or routine use), employed security, restrictions of further use, information about disposition, and a cost-benefit analysis.

Suggestion: Implement proper procedures for Computer Matching, where required.

TLA may occasionally deal with data at Sensitivity Level 4 or classified data

Unauthorized access to or compromise of information with Sensitivity Level 4 "could result in severe mission capability degradation, major damage to DoD information based resources, or a risk of serious injury or death to personnel." A sufficiently large breach of TLA data will likely rise to this level of sensitivity. Moreover, certain specific qualifications, assessments, or training activities may themselves bear this level of sensitivity, or even be deemed "classified".

Data may only be classified by the Secretary of Defense, the Secretaries of the Military Departments, Senior Agency Officials, and specific delegates (DoD 5200.1-R, section 2.2). The following type of information may be classified (DoD 5200.1-R, section 2.3.2):

- Military plans, weapon systems or operations.
- Foreign government information.
- Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- Foreign relations or activities of the United States, including confidential sources.
- Scientific, technological or economic matters relating to the national security.
- United States Government programs for safeguarding nuclear materials or facilities.
- Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Suggestion: The TLA infrastructure must be prepared to handle classified information.

Beyond these suggestions, NIST guidelines may be used to determine the Sensitivity Level of TLA data

NIST SP 800-122, Section 3.2 outlines a number of factors that can be used to determine the impact from a loss of confidentiality of PII. While these factors were developed to determine the "PII Confidentiality Impact Levels" outlined in the Federal Information Processing Standards publication on "Standards for Security Categorization of Federal Information and Information Systems" (FIPS 199), they can also be used to determine the Sensitivity Level of TLA data.

- Identifiability: The Sensitivity Level of TLA data should be evaluated with respect to the ease with which it can be used to identify specific individuals. For example, an SSN uniquely and directly identifies an individual, whereas a telephone area code identifies a set of people (NIST SP 800-122, Section 3.2.1).
- Quantity of PII: The Sensitivity Level of TLA data should be evaluated with respect to how many individuals can be identified from the PII within TLA. For example, breaches of 25 records and 25 million records may have different impacts. However, the Sensitivity Level should not lowered simply because the number of records is small (NIST SP 800-122, Section 3.2.2).
- Data field sensitivity: The Sensitivity Level of TLA data should be evaluated with respect to the sensitivity of each individual data field that comprises the data. For example, an SSN is generally more sensitive than a phone number. This evaluation should a2so consider the additional sensitivity incurred when data fields are combined (NIST SP 800-122, Section 3.2.3).
- Context of use: The Sensitivity Level of TLA data should be evaluated with respect to the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The same data may be assigned a different Sensitivity Level based on their use (NIST SP 800-122, Section 3.2.4).
- Access and location: The Sensitivity Level of TLA data should be evaluated with respect to the nature of authorized access and the potential off-site storage and/or transportation of the data. This is not to suggest that data should be given a lower Sensitivity Level to expedite these processes. Rather, data that is regularly stored, transported, and/or accessed on devices not under the control of DoD should be assigned a higher Sensitivity Level.

Suggestion: Follow the NIST guidelines to determine the Sensitivity Level of TLA data if the Sensitivity Level is not otherwise prescribed.

Devices and authentication

DoDI 8520.03, section 4 describes that "the specific environment (i.e., the connectivity medium and the computer) from which any entity may initiate an authentication session must be considered when selecting the appropriate or required identity credential for identity authentication to a system or network by a user or group of users."

Five unclassified entity environments are described:

- DoD Network: owned and operated on behalf of the DoD, physically connected to a DoD unclassified network, and physically located on DoD premises.
- DoD Managed: owned or operated on behalf of the DoD but not physically connected to a DoD network. Logon to a DoD unclassified network from a DoD managed environment must use technologies (e.g., VPN) approved for use in applicable STIGs.
- Partner Managed: owned and managed by a DoD mission partner and not physically connected to a DoD network.
- User Managed: a personally owned computing asset.
- Untrusted: cannot be as being under the management or control of the DoD, mission partner, or individual.

The "entity environment" determines the minimum credential strength required for accessing information systems with various levels of sensitivity (DoDI 8520.03, section 5).

Routine use of TLA may happen with DoD authorized devices, using single-factor authentication

Most TLA data can be considered at Sensitivity Level 1 (see "Sensitivity levels of data"). At this level, data may be accessed from untrusted devices, however, DoD 5400.11-R, section AP1.5.5 suggests that "only DoD authorized devices shall be used for remote access." These remote devices must conform to the Information Assurance (IA) controls outlined in DoDI 8500.2. Access to data at Sensitivity Level 1 requires minimal Credential Strength A.

Suggestion: It should be permissible to access TLA for routine uses with any DoD authorized device that conforms to IA controls, via all DoD or partner managed environments, and via any DoD network. Users should be authenticated using Credential Strength A. This entails an authentication method at Authenticator Assurance Level 1 (i.e., single-factor authentication, such as a password). Re-authentication is required at least every 30 days (NIST SP 800-63-3B).

Certain types of TLA access are not allowed from untrusted devices and require a higher credential strength

Learning materials that are either proprietary or confidential (e.g. test materials) are considered to be at Sensitivity Level 2 (see "Sensitivity levels of data"). Such data cannot be accessed from an untrusted device and require a higher credential strength (unless they are accessed from a DoD network). Particularly, in a DoD managed or partner managed environment, such access requires Credential Strength B, and on a user managed device it requires Credential Strength D.

Moreover, access to "personnel management data" (i.e., substantial amounts of TLA data from multiple users) is considered to be at Sensitivity Level 3, which requires an even higher credential strength. Particularly, on the DoD network it requires Credential Strength B, in a DoD managed or partner managed it requires Credential Strength C, and on a user managed device it requires Credential Strength D.

Credential Strength B requires Authenticator Assurance Level 2 (multi-factor authentication without PKI, or two types of single-factor authentication where one is memorized and the other is possession-based), Credential Strength C requires Authenticator Assurance Level 3 (multi-factor authentication with PKI), and Credential Strength D requires Authenticator Assurance Level 3 with the specific use of a hardware token PKI technology (NIST SP 800-63-3B). At these strengths, reauthentication is mandated after 12 hours, or when a session is inactive for more than

30 minutes (AAL2) or 15 minutes (AAL3) (NIST SP 800-63-3). Moreover, at these strengths, the credential service provider must be audited by a third party at least once every 3 years to ensure compliance with its documentation (NIST SP 800-63-3).

Suggestion: TLA-based systems should implement multi-factor authentication (with PKI) for access to certain learning materials and "personnel management data" on DoD networks and in DoD or partner managed environments. Moreover, they should implement hardware token authentication for access to such data via user managed devices. Finally, they should deny access to such data via untrusted devices. In all of these cases, re-authentication should be required after 12 hours and after 30 minutes (AAL2) or 15 minutes (AAL3) of inactivity.

Use of data at Sensitivity Levels 1, 2 and 3 requires an intermediate level of identity verification

NIST outlines three Identity Assurance Levels, the middle of which is most suitable for regular TLA authentication purposes (i.e., for use of data at Sensitivity Levels 1, 2 and 3). It allows remote identification using a single piece of "superior" identity evidence that has been confirmed by biometric comparison or two pieces of "strong" identity evidence. For more details, see NIST SP 800-63-3A. DoDD 8521.01E encourages the centralized collection and use of biometric data for identification purposes. The collection and use of biometric data is itself subject to the regulations stipulated in the DoD Privacy Program (DoDD 5400.11).

Suggestion: The identity of users with access to data at Sensitivity Levels 1, 2, and 3 should be verified at IAL2 (see NIST SP 800-63-3A).

TLA can federate authentication to non-confidential learning activities using an intermediate level of federation assurance

Once users are authenticated in TLA, the TLA infrastructure can federate authentication to its learning activities. NIST outlines three Federation Assurance Levels, the middle of which is most suitable for regular TLA authentication purposes (i.e., for use of data at Sensitivity Levels 1, 2 and 3). It requires TLA to sign the assertion and to encrypt it using the public key of the learning activity (to ascertain authenticity). For more details, see NIST SP 800-63-3C).

Suggestion: The TLA infrastructure can federate authentication to non-confidential learning activities using FAL2 (see NIST SP 800-63-3C).

Additional requirements exist for administrative access and access to classified data

Access to a sufficiently large part of the TLA infrastructure — usually characterized as administrative access — requires authentication at Credential Strength E. Moreover, classified data can only be accessed via a classified environment, which has its own Credential Strength classifications.

On top of a hardware token PKI technology (NIST SP 800-63-3), Credential Strength E requires that the user's identity has been proofed and vetted in accordance with FIPS 201-2, and that the credential service provider is a Federal agency, approved under the Federal PKI Policy Authority Program, or approved by the DoD CIO. For classified data access, credential providers must be a member of or cross-certified with the NSS PKI or approved by the DoD CIO.

Suggestion: TLA-based systems should make sure that administrators are vetted in accordance with FIPS 201-2. Moreover, they should make sure that classified data can only be accessed from classified environments using verified credential providers and biometric identification mechanisms. Identity verification methods should be assured at level 3 (see NIST SP 800-63-3A).

Administrative access and access to classified data requires a high level of identity verification

Only the highest NIST Identity Assurance Level is suitable for administrative access and access to classified data. IAL3 requires in-person or supervised remote identification using multiple pieces of "superior" identity evidence that has been confirmed by biometric comparison. For more details, see NIST SP 800-63-3A.

Suggestion: The identity of users with administrative access and/or access to classified data should be verified at IAL3 (see NIST SP 800-63-3A).

TLA must use a high level of federation assurance to federate authentication to learning activities that handle classified data and to federate authentication for administrative access

Only the highest NIST Federation Assurance Level is suitable for federated authentication to learning activities that handle classified data. The same is true for federated authentication for administrative access to a learning activity. Like FAL2, FAL3 requires TLA to sign the assertion and to encrypt it using the public key of the learning activity (to ascertain authenticity). Additionally, the user must present a cryptographic key (cf. PKI). For more details, see NIST SP 800-63-3C).

Suggestion: The TLA infrastructure must federate authentication to learning activities that handle classified data and to federate authentication for administrative access using FAL3 (see NIST SP 800-63-3C).

Violations and review

Data accuracy

Data must be accurate, timely and complete, even after a computer failure

DoD components should make sure that data is "accurate, timely, complete and relevant before disclosure" (DoD 5400.11-R, section 4.1 and OMB M-07-16). If there is a computer failure, they are also responsible for restoring all protected information to ensure data integrity (DoD 5400.11-R, section AP1.3.6).

This requirement must be traded off with privacy and data security: data integrity can be improved using caching and redundancy, but these mechanisms result in additional vulnerabilities.

Suggestion: TLA should use caching and redundancy to improve data integrity but at the same time make sure to properly protect these systems against security threats and privacy violations. Other integrity-improving mechanisms include the use of fault-tolerant RAID array storage and transactional database systems.

Reports and inspections

TLA-based systems must comply with requests for reports and inspections

The DoD CIO has established mechanisms to facilitate organizationally tiered compliance reviews for IT investments to ensure compliance with enterprise architectures, privacy requirements, and IT standards (DoDD 8000.01, enclosure 2, paragraph 1f). In line with these mechanisms, DoD components are required to provide data for reports prepared by the DPO (DoD 5400.11-R, chapter 8) and are subject to inspection for compliance with regulations (DoD 5400.11-R, chapter 9).

Suggestion: TLA-based systems should employ automated reporting mechanisms to support DPO reports and inspections.

Violations

> *Loss, theft, or compromise of PII must be reported to US CERT and the Senior Component Official for Privacy*

Loss, theft or compromise of PII shall be reported to US CERT within 1 hour, and to the Senior Component Official for Privacy within 24 hours (DoD 5400.11-R, section 10.6). Reports must include:

- Component or organization involved.
- Date of the event.
- Number and classification of affected individuals.
- Facts and circumstances e.g. timeliness, source, content and means of providing notification.
- Actions taken to mitigate the effects.
- Who received the notification; public outreach response.

OMB M-07-16 requires federal agencies have a proactive plan for handling breach notifications. This plan must include the mentioned reporting elements.

Suggestion: TLA-based systems should have a technical mechanism to efficiently report the requisite information US CERT and the Senior Component Official for Privacy in case of violations. This technical mechanism should implement the organization's breach notification plan.

> *In case of loss, theft, or compromise, the affected individuals must be notified within 10 days*

Individuals should be notified within 10 days (but as soon as possible) when any records containing personal information are lost, stolen, or compromised. This 10-day window begins after the Component is able to determine the identities of those affected (DoD 5400.11-R, section 1.5). If only some but not all affected individuals can be identified, "notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified." If affected individuals cannot be readily identified or they will not be able to be identified, "the Component shall provide a generalized notice to the potentially impacted population by whatever means is most likely to reach the affected individuals."

If a breach happens at a contractor, the contractor must notify the Component of the breach immediately upon discovery. The Component shall then determine whether the Component or the contractor shall make the required notification. If the contractor makes the notification, it must be reviewed and approved by the Component.

The notice to the affected individuals should include, at a minimum:

- What specific data was involved.
- The facts and circumstances surrounding the loss, theft, or compromise.
- What protective actions the Component is taking, or the individual can take to mitigate against potential future harm.

NIST guidelines (NIST SP 800-122, section 5.1) make the following suggestions regarding the coordination of responses to potential breaches:

- Organizations should establish a committee or person responsible for coordinating the breach response.
- Organizations should determine how breach incidents are tracked within the organization.
- Organizations should determine what circumstances require the provision of remedial assistance to indivduals (e.g. credit monitoring services).

Suggestion: TLA-based systems should have a technical mechanism and standardized procedures to notify TLA users of violations and to track violations within the organization. Each system should have a designated person or committee responsible for coordinating the response to potential breaches.

Conclusion

This document has outlined how existing privacy regulations and recommendations are applicable to TLA-based systems. In short, the following recommendations are made:

The legal **scope of privacy** is such that TLA-based systems should assume that all collected data can potentially be classified as Personally Identifiable Information (PII) and that all learning activities are therefore subject to the privacy protection responsibilities outlined in this document. As TLA is a distributed architecture, system capabilities should be developed (e.g. an API) that can manage the processing of PII in accordance to regulations for both "disclosure within the DoD" as well as disclosures to and from "third parties".

TLA-based systems should also follow guidelines of the DoD Information Security Program for **safeguarding data**; this includes physical safeguards (regulate physical access to TLA systems, proper erasure/disposal of data, and the use of authorized devices), technical safeguards (a combination of strict access control, encryption, de-identification and obfuscation), and management procedures (a tool to manage access authorizations).

Special procedures are recommended for **onboarding learning activities**. This includes training all TLA users, developers, and managers; conducting a privacy evaluation / impact assessment; and publishing their privacy practices as a system notice and a Privacy Act statement to the Federal Register (where required). The system notice should be a requirement to become an authorized component of the TLA infrastructure. The infrastructure itself should publish a match notice for authentication purposes.

Given DoD rules, the TLA infrastructure and/or activity providers must ask users for consent to gain **access to personal information**. This request must be accompanied by a Privacy Act statement, which can be automatically generated from the Federal Register. The statement should be "textured" and displayed in close proximity to the actual information request. Once access is authorized, it does not have to be re-authorized unless the stated purpose or routine use of the information change. Disclosures must be scrutable by the users to whom they apply. Likewise, users must be able to access and amend the data collected about them. Collected data can be published more broadly following the guidelines outlined in DoDI 8550.01.

Regarding **data, devices and authentication**, following NIST guidelines, most TLA data is considered Security Level 1, although learning materials are Level 2, aggregate data can be considered Level 3, and certain data may be Level 4 or even classified. Accordingly, most routine use requires single-factor authentication and intermediate level identity verification. More sensitive data may require a higher credential strength, may be restricted to trusted devices, and may require more robust identity verification. TLA can federate authentication but must do so using the appropriate credential strength (depending on the type of access given at the learning activity level).

TLA-based systems should employ semi-automated technical mechanisms to handle **violations and review** requests. This allows the system to notify CERT (within 1 hour) and affected users (within 10 days) in case of a data breach.

We note that these guidelines are non-exhaustive, as they are based on a thorough but not comprehensive review of the legal landscape.

References

Shorthand code	Full title and URL
DD Form 2930	Privacy Impact Assessment https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2930.pdf
DoD 5200.1-R	Information Security Program https://www.hsdl.org/?view&did=506
DoD 5400.11-R	Department of Defense Privacy Program https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/540011r.pdf

DoDD 5400.11	DoD Privacy Program https://www.hsdl.org/?view&did=469495
DoDD 8000.01	Management of the Department of Defense Information Enterprise https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf
DoDD 8521.01E	DoD Biometrics https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/852101E.pdf
DoDI 1000.30	Reduction of Social Security Number (SSN) Use Within DoD https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/100030p.pdf
DoDI 5400.16	DoD Privacy Impact Assessment (PIA) Guidance https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540016p.pdf
DoDI 7750.07	DoD Forms Management Program https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/775007p.pdf
DoDI 8500.1	Cybersecurity https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
DoDI 8500.2	Information Assurance (IA) Implementation https://fas.org/irp/doddir/dod/d8500_2.pdf
DoDI 8520.03	Identity Authentication for Information Systems https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf
DODI 8550.01	DoD Internet Services and Internet-Based Capabilities https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855001p.pdf
DoDI 8910.01	Information Collection and Reporting https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/891001p.pdf
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
GAO report 08-536	Alternatives Exist for Enhancing Protection of Personally Identifiable Information https://www.gao.gov/new.items/d08536.pdf
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
NIST SP 800-63-3	Digital Identity Guidelines https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
NIST SP 800-63-3A	Digital Identity Guidelines: Enrollment and Identity Proofing https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
NIST SP 800-63-3B	Digital Identity Guidelines: Authentication and Lifecycle Management https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
NIST SP 800-63-3C	Digital Identity Guidelines: Federation and Assertions https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf
OMB M-06-19	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-19.pdf
OMB M-07-16	Safeguarding Against and Responding to the Breach of Personally Identifiable Information https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
OMB M-10-22	Guidance for Online Use of Web Measurement and Customization Technologies https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-22.pdf
PS4TLA Spec 4	Privacy Support for the Total Learning Architecture: Privacy Recommendations

	https://adlnet.gov/projects/ps4tla/
Public Law 107–347	E-Government Act of 2002 https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
USC title 44, chapter 35	Coordination of Federal Information Policy https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter35&edition=prelim
USC title 5, section 552a	Privacy Act of 1974 https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title5-section552a&edition=prelim