INTERIM GUIDANCE: CC SRG update WRT PII/PHI in the Cloud and PII at IL2

NOTICE: The following is a snippet from a forthcoming update to the CC SRG provided here to provide context for the DoD CIO memo dated 7 August 2019 "Treatment of PII within Level 2 Commercial CSOs for DoD". This replaces 5.1.5 and 5.1.5.1 in the reorganized section 5.1.5. The information on the Privacy overlay follows these sections in the CC SRG.

5.1.5 Personally Identifiable Information (PII) / Protected Health Information (PHI) in the Cloud

Personally Identifiable Information (PII) and Protected Health Information (PHI) are categorized as CUI and as such PHI and most PII in the cloud must minimally be protected in a Level 4 CSO. Most PII means PII categorized as having a Moderate or High (and some Low not meeting the exception below) confidentiality impact level as determined in accordance with *NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[1].

Mission Owner PII impact level determinations will be performed as part of the information system's Privacy Impact Assessment per DoD Instruction 5400.16, "*DoD Privacy Impact Assessment (PIA) Guidance*"[2] and documented in Section 2.b. of DD Form 2930 "*Privacy Impact Assessment (PIA)*[3]. This determination will take into account all relevant factors as presented in Section 3.2 of NIST SP 800-122 and guidance for assessing the risk of harm to individuals potentially affected by a breach in Section E of OMB Memo 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"[4].

Mission Owners will publish, collect, process and store all sensitivity levels of PII in coordination with, and the approval of, their DoD Component's senior privacy officer or their delegate.

5.1.5.1 PII at Level 2

It is recognized that there is a need for some low confidentiality impact (low sensitivity) PII to be published or collected in commercial CSOs having a Level 2 PA. DoD CIO memo dated 7 August 2019, "Treatment of PII within Level 2 Commercial CSOs for DoD" states that "Level 2 will be the minimum cybersecurity requirement for DoD systems/applications containing Low confidentiality impact level PII as determined in accordance with NIST SP 800-122".

NOTE: A DoD Information Impact Level 2 PA is based on the FedRAMP Moderate Baseline, thus PII at Level 2 will be protected at the moderate level IAW 32 CFR 2002 Controlled Unclassified Information[5].

---

[1] NIST SP 800-122: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
[2] DoDI 5400.16: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540016p.pdf
[3] DD Form 2930: https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2930.pdf?ver=2017-08-11-145827-790
[4] OMB Memo 17-12: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
[5] 32 CFR 2002 CUI: https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

The following requirements are provided for Low PII published, collected, stored, or processed in commercial CSOs:

- Mission Owners will only publish, collect, store, process low confidentiality impact (sensitivity) PII in a CSO minimally possessing a FedRAMP Moderate P-ATO listed on the FedRAMP Marketplace and a DoD Level 2 PA, with Privacy Officer approval.
- Mission Owner PII impact level determination will consider all relevant factors together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor.
- Prior to authorizing the system, the AO is accountable to review the PIA and ensure that appropriate cyber assessments are performed per DoDI 8510.01, the CC SRG, and that required CSSP cybersecurity support services are provided per DoDI 8530.01.
- Low impact/sensitivity PII when published or collected in a CSO with a Level 2 PA must be minimally protected in accordance with NIST SP 800-122 and privacy laws as supported by a FedRAMP Moderate P-ATO, and the Low PII overlay of the Privacy Overlay (see Section 5.1.5.2, CNSSI 1253 Privacy Overlay).

NOTE: Authentication and identification information of privileged users required for the configuration, operation, and maintenance of the IL2 CSO and Mission Owner's application is exempt from the above requirements providing it is protected as all such information is customarily protected.