Security Enhancements

PSB Requirements

A product security baseline requirement is a security standard that

- establishes minimum security measures for software and systems,
- aligns with product security features for each release, and
- ensures compliance across essential security domains.

These are the main complaince categories:

- TPS management and vulnerability handling
- Threat modeling and security testing
- Security features and protections
- Documentation and system processes

PCRF PSB requirements

CPS supports these PSB requirements:

Table 1: PSB Requirements

PSB Item	Description
CT2340: SEC-UPS-TPSQUAL-FR1-v3	Remove any TPS component present in the Corona Exclusion List (COR-EL).
CT2337: SEC-UPS-TPSQUAL-FR2-v3	Review high-risk vulnerabilities to determine their applicability to the offering.
CT2349: SEC-UPS-TPSQUAL-FR3-v3	Fix TPS vulnerabilities within the documented timelines.

PSB Item	Description
CT2354: SEC-UPS-TPSQUAL-FR4-v3	Respond to CVR Disposition Requests (DR) within the documented timeline.
CT2336: SEC-UPS-REGI-FR1-v5	Register Third-Party Software.
CT2335: SEC-UPS-REGI-FR2-v5	Update TPS Registrations regularly.
CT2330: SEC-ASU-TMOD-FR1-v4	Create and Review a System-Level Threat model.
CT2329: SEC-ASU-TMOD-FR2-v4	Assess and Mitigate Threats Against High-value assets.
CT2321: SEC-ASU-TMOD-FR3-v4	Create Additional Threat Models for new features.
CT2326: SEC-ASU-TMOD-FR4-v4	Update Threat Models as needed.
CT2322: SEC-ASU-TMOD-FR5-v4	Threat Model review.
CT2325:SEC-ASU-STATIC-4	Perform Static Application Security Testing ([SAST](/library/glossary/CG181)).
CT2339: SEC-WEB-CSRF-4	Prevent CSRF vulnerabilities.
CT2324: SEC-AUT-DEFROOT-3	No default credentials.
CT2323: SEC-DAT-KNOWWHAT-3	Know and document what data your product or service processes and assess the legal, security, and privacy risk.
CT2347: SEC-UPS-REGI-FR3-v5	Create a Distribution-Ready Software Bill of Materials (SBOM).
CT2353: SEC-UPS-UPDATE	Update Third-party Software (TPS) Components regularly.
CT2346: SEC-FOR-DEBUG	Provide secure root/admin access for forensic analysis.
CT682: SEC-CON-PERM	Filter incoming connections by source IP address
CT2327: SEC-ASU-TMOD-FR6-v4	Store Threat models
P8: CT2236: SEC-SW-APPDTCT-FR5-v1	Check all signatures before loading code.
P8: CT2238: SEC-SW-APPDTCT-FR7-v1	Cisco-controlled Authentication roots.
CT2237: SEC-SW-APPDTCT-FR6-v1	Load Verification Trust Chain for Closed code.
CT1890: SEC-NTP-AUTH	Support NTP, NTP authentication, and filtering.
CT2301: SEC-IP-IPv6-2	Support all security requirements over IPv6.

vDRA PSB requirements

CPS supports these PSB requirements:

Table 2: PSB Requirements

PSB Item	Description
SEC-VAL-INEVAL-2	Prevent injection vulnerabilities by not passing uncontrolled data to other Execution Spaces.
SEC-VAL-INXPATH-2	Use prepared statements or validate user input to construct XPath queries.
SEC-VAL-INXXE-2	Disable entity expansion or validate text content after expansion to prevent XML eXternal Entity (XXE) Injection.
SEC-WEB-RESP-3	Specify type and encoding in HTTP responses; disable type sniffing.
SEC-CRY-PRIM-9	Use approved cryptographic primitives and parameters.
SEC-CRY-STDCODE-FR3-v3	Third-Party Libraries.
SEC-TLS-CURR-6	TLS 1.2 and TLS 1.3.
SEC-DAT-KNOWWHAT-3	Know and document what data your product or service processes and assess the legal, security, and privacy risk.
SEC-SCR-CONFLEAK-3	Do not expose critical data
SEC-CRY-ALWAYS-3	Provide cryptographic protection outside controlled space
SEC-ASU-TMOD-4	Create and Review a System-Level Threat Mode
SEC-ASU-TMOD-FR1-v4	Create and Review a System-Level Threat Model.
SEC-ASU-TMOD-FR2-v4	Assess and Mitigate Threats Against High-value assets.
SEC-ASU-TMOD-FR3-v4	Create Additional Threat Models for new features.
SEC-ASU-TMOD-FR4-v4	Update Threat Models as needed.
SEC-ASU-TMOD-FR5-v4	Threat Model review
SEC-ASU-SCAN-3	Evaluate the attack surface of an operational offering using automated scanning tools
SEC-UPS-REGI-FR1-v5	Register Third-Party Software
SEC-UPS-REGI-FR2-v5	Update TPS registrations regularly.
SEC-UPS-TPSQUAL-FR2-v3	Review high-risk vulnerabilities to determine their applicability to the offering

PSB Item	Description
SEC-UPS-TPSQUAL-FR3-v3	Fix TPS vulnerabilities within the documented timelines.
SEC-UPS-TPSQUAL-FR4-v3	Respond to CVR Disposition Requests (DR) within the documented timeline.
SEC-RUN-ASLR-FR1-v3	Randomize memory segments.
SEC-RUN-ASLR-FR2-v3	Randomization Entropy.
SEC-RUN-ASLR-FR3-v3	ASLR can not be disabled