|  |
| --- |
| Attacks & S/w Vuln: Attacks: **XML attacks** (targets app that parses/reads/interprets XML. If contains reference to external entity (XXE), weak parser leads to disclosure of confidential data, DoS, SSRF, port scanning); *Mitigation*: **XACML** (create attribute-based access control, used across apps, decouples access decisions from app or local machine; fine-grained based on: attributes of user requesting access, protocol of request, authn mechanism; XACML uses **policy enforcement point** (PEP, protects resource that subject or app attempting to access, makes XACML req) and **policy decision point** (PDP, retrieves policies in XACML & compares with its policies, responds to PEP).) | **SQLi** (can be identified in logs using *Log Parser* (CLI, SQL-like cmds, search/locate errors) by Microsoft.) | **overflow attacks** (occurs when memory area is full and cannot hold more info; overflown info is lost; attackers use overflow to permit impermissible actions; **buffer** is area of memory used to transfer data across locations; **1. buffer overflow**: data submitted is more than it can handle; poorly written app/os code; results in injection of malicious code/DoS/SQLi; *Mitigation*: latest update, service packs/ patches; test for overflow conditions; **NOP slide**: long string of NOP followed by cmd, leading to buffer overflow; purpose is get CPU locate where cmd to be executed; **2.** **Integer overflow**: math operations create numeric value too large for available space; A signed int (normally +ve), can become -ve with overflow; *Mitigation*: strict i/p validation, use lang or compiler that performs automated bounds checks, choose int type that contains possible values of calculation; then no need for **integer casting** (changing datatype)); **3.** **Heap**: increase or decrease in memory size; sits b/w memory-mapped region & runtime heap; called **dynamic memory allocation**;| **RCE** (Victim’s local/user system executes code from hacker that resides on another machine located anywhere; sometimes embedded in websites user visits; code injected in user’s browser;) | **Directory Traversal** (break out of web root, access restricted directories, execute cmds; *Mitigations*: i/p filtering, remove metacharacters.)| **Priv esc** (get access that is not entitled; delete files, view private info, install unwanted programs/virus; 2 types: **1. Vertical priv esc** (low-priv user/app access high-priv user/app) & **2.** **Horizontal priv esc**: (one user access other user’s data); *Mitigation*: DB/systems/app are operating w/ minimal priv to function; users given min priv for job; DB doesn’t run as root or admin) |**Pwd spraying** (form of brute-force; to identify pwd of domain users; spray multiple accts w/ same pwd; can avoid acct lockout by waiting in between attempts) | **Cred stuffing** (form of brute-force; re-use stolen user/pwd combination on another website/service; ***Mitigation***: Implement MFA, check compromised accts & reset pwd if user appear on list; periodic pwd resets; CAPTCHAs) | **Impersonation** (one user acquire identify of other by logon creds; by social eng, or sniffing; *Mitigation*: user education) | **MITM** (intercepts traffic between systems; **ARP spoofing :** poison ARP cache on switch by answering ARP req from another IP address but own MAC addr; *Mitigation*: **Dynamic ARP inspection** (**DAI**) [compare w/ trusted ip-mac list; switch rejects packet on incorrect mapping], **DHCP snooping** [prevent poisoning DHCP database; map of IP-MAC from trusted DHCP server; *DAI depends on DHCP snooping*; can implement both mitigations])| **MAC overflow** (fill switch’s MAC table with nonexistent MAC addr; prevents valid devices creating **CAM** entries; hacker then captures all traffic) | **VLAN-based attacks** (**1.** **Switch spoofing**: can use DTP (Dynamic Trunking Proto) to form a trunk line; hacker sets interface to spoof switch/ use DTP to create trunk line; *Mitigation*: Disable DTP on switch ports; Switch ports hardcoded to trunk or access | **2.** **Double tagging**: (tags identify VLAN frames; **VLAN hopping** can be done using double tagging;))| **Session hijack** (MITM; *Juggernaut*, *Hunt Project* allows spying TCP; DoS to remove one system, & spoof IP of it; takeover sesion) | **Rootkit** (set of tools to use after gaining admin access; hardest to remove; needs reformat drive; Actions by rootkit: 1. Install backdoor; 2. Remove entries from security log (**log scrubbing**);3. Replace with trojans, 4. Malicious kernel changes; *Mitigation*: monitor system memory for processes; MS safety scanner for hidden info from Win API, MFT, Directory index; Use Malwarebytes Anti-Rootkit 2019; Firewalls updated; Harden workstations)| **XSS** (Reflected (non-persistent or Type-II); Persistent (stored or Type-I); DOM-based (Type-0), source/sink/data - all in DOM) | Vulnerabilities: Improper error handling, dereferencing (null-pointer used as pointed to valid memory; Throws **null-pointer exception**; debug info obtained), insecure direct object reference (Authz issue; code review needed), **race condition** (targets normal sequence of functions; hackers inserts to alter order of execution; e.g. Time-of-check/time-of-use vuln; *Mitigations*: **atomic** [run in entirety or prevent changes]; Lock access to certain items when program is running;), broken authn (guess pwd, crack pwd hash, social engg like shoulder surfing; CVSS has H (needs admin), M (basic user priv on settings & files), L (no authn in place to stop exploit)), sensitive data exposure (usernames, pwds, encryption keys, ), insecure software components (DHS estimate 90% of reuse from code repo; CVE), insufficient logging & monitoring, weak/default config, use of insecure functions |
| S/w Assurance Best Practices: **Containerization**: newer feature of mobile device management (MDM) software that creates an encrypted “container” to hold & quarantine corporate data separately from that of the user’s data|[MDM **configuration profiles** (w/ **payloads** settings) are used to control the use of devices; **POCE** (**personally-owned, corporate-enabled**) devices are managed by MDM software; **COPE** (**corporate owned, personally enabled**): org purchases, users manage; COPE gives company power on policy and protecting devices;] [**Application wrapping**: protect mobile devices w/ policies like authn req/app data storage; allows safely download an app from store;] [**Conditional access**: fine-grained policies that control access to data based on conditions of conn, user, location, device state, app sensitivity, real-time risk;] [**Remote wipes**: instructions to erase data in lost/stolen case; part of MDM s/w; consent from user is required;] [**SCEP** (Simple Certificate Enrollment Protocol): certs to n/w & mobile devices; Uses Manual (wait for CA to approve) & Pre-shared secret (challenge pwd, delivered out-of-band; returned to server; Do not use for device authn) as authn for enrollment;] [**NIST SP 800-163 Rev 1**: **Vetting security of mobile apps**: [**1. App vetting** (seq of activity to confirm org’s sec req), **2. App intake** (app received for analysis; manual by admin/automated by vetting system; two i/p: app considered (req), testing artifacts(reports f/ previous results)(optional)), **3. App testing** (app registered; preprocessed; forward to test tool; chk for vuln), **4. App approve/reject** (after vuln & risk report; sec analyst inspects for sec reqs), **5. Result submit** (after validation by AO, prepare artifacts for submission), **6. App re-vetting** (updates/threats treated as new s/w; depends on risk tolerance)];] [**Maintenance hook**: set of instructions in code to allow backdoor conn to view/edit code without normal access controls (security issue if known to hackers); *Mitigation*: Use HIDS to record hook access; Encrypt data on system; Audits on IDS; Remove hooks before going to prod;] [**Time-of-check/time-of-use attacks**: seq of events; depends on knowledge of dependencies; **race condition**: attacker inserted b/w instructions, make changes, alters order of execution & outcome: *Mitigations*: atomic instructions, must execute in order or rollback or prevent; lock access when running instructions] [**CSRF** (exploit website’s trust of browser); *Mitigation*: URLEncode, HTMLEncode, on params w/ special chars; **Click-jacking**: transparent page/frame over legitimate page that users clicks to grab creds;] [**Embedded**: dedicated function within large system; real-time computing constraints; in cars; HVAC; alarms; lighting; M2M; IoT; **security not built-in;** manuf comm to internet for diagnosis can lead hacker to reverse comm and take over] [**System-on-Chip** (SoC): integrated circuit of all PC components or another electronic system; built on microprocessor; *Secure SoC*: **Secure booting** -> series of authn process on h/w & s/w used in boot chain;; starts from trusted entity (anchor point); *security-breach-response* unit monitors intrusions; **Firmware**: s/w on erasable programmable read-only memory (**EPROM**) or **EEPROM** (electrically erasable POM, f/w is often installed here) chip on device; exist as BIOS on computer/device. Neglected updates: “*if it ain’t broke, don’t fix it*”; most updates are security related; PCs & batteries has lot of firmware: usb, webcams, graphics, sound cards] [**SDLC steps**: 1.Plan/initiate project, 2.Gather reqs, 3.Design (desc of s/w func & sec goals; **state** of the app refers to its functional & security posture during each operation it performs; identify attack surface), 4.Develop, 5.Test (orig design spec met)/validate (high-level view, orig s/w purpose met);6.Release/maintain, 7.Certify (evaluate s/w for security effect w/ customer needs)/accreditation (formal acceptance by mgmt. on system security), 8.Change mgmt. & config mgmt.] [**DevSecOps**: actors in DevOps: Dev, QA, Ops; *Plan,Code,Build,Test,Release,Deploy,Operate,Monitor*; **Stress test order**: step-1.Identify test obj; 2.key scenarios, 3.workload to apply, 4.metrics to collect, 5. Test cases, 6.simiulate load, 7.analyze results] [**Security Regression Testing**: verify func after changes to s/w; subset of regression; *Steps*: *single unit regression* | *partial regression* (new code with old code)| *complete regression* (test on all units);][**Code Review**: systematic investigation of code for security & functional problems; *2 types*: Formal review (extremely thorough, line-by-line) & Lightweight review (pair programming, email review, over the shoulder, tool-assisted); **Code review process**: Fagan inspection: *Plan*-*Overview*-*Prepare*-*Inspect*-*Rework*-*Follow-up*] [**Security Testing**: Blackbox/Zero-knowledge/closed testing | Whitebox | Greybox] [**Secure coding best practices**: I/p validation (Blacklisting [character / pattern to block], Whitelisting), O/p encoding (URL encode % sign, Unicode), Session mgmt.(desktop & remote sessions), NO AUTHN = NO SECURITY and NO ACCOUNTABILITY; **Context-based authn**: attribute-based: time, location, frequency, behavior] [**SOA**: distributed computing model; removes redundant code per app; s/w best practice due to **service brokers**;] [**SAML**: XML+SOAP] [**SOAP**: exchange structured info in webservices; SOAP processing model (rules); SOAP extensibility model (features/modules); SOAP binding framework (exchange message b/w nodes); SOAP message; *Disadvantage*: verbosity] [**REST**: client/server model w/ HTTP; no specific message format; XML or JSON; REST/JSON better: Size, Efficiency, Caching, Implementation; **SOAP/XML is used in banking transactional service**.] [**SOA microservice**: self-contained piece w/ business functionality, variant of SOA structural style & arranges app as collection of loosely coupled services, single-function modules /w interfaces & ops] |
| IR process & Apply IR best practices: [Communication Plan: (**Benefits**: control on process/goals of IR achieved; **Failure**: Lawsuits, premature alert of suspect, sensitive info disclosure, less effective IR | Limit comm to trusted parties | Disclose based on regulatory/legislative req | Prevent in-advert release of info | specific method of comm. (out of band like **off-the-record (OTR) messaging**) | Reporting reqs (HIPPA breach notif Rule 45 CFR 164.400-414: PHI; 50 states mandating PII notif)] [Resp coordination Different entities: (**legal** (NDAs, wording of docs to contact sites/orgs, assess liability), **HR** (job desc of IR hiring, policy/proc to remove empl in illegal activity), **Public relation** (manage dialog b/w org and outside world; 1 person designated to media; consistent message; handle press conf, written resp to outside world), Internal & External (**law enf** (**USA PATRIOT Act**: enhanced IR tools, ability to look at emails, phone records, internet comm, medical records, financial records), industry orgs, media), Senior leadership (support verbal & financial; comm to all org; agreements to authority of IR team; decision systems for key changes in network), Regulatory bodies) ] [ Data criticality: **PII** (*full name, IDs, DoB, place of birth, biometric data, financial acct nbrs, digital IDs*) -> GDPR; **PHI** -> **HIPPA;** **SPI** (Sensitive Personal Info): creditcards -> PCI-DSS (3.2.1, not law but std); High value assets or Critical systems (that provide access to info); Financial & accounting data is in **Accounting Info systems (AIS)**; **Protect financial info**: physical security, firewall, audit perm, encrypt data, backup data w/ RAID; {**IP (Intellectual property)**: (tangile / intangible asset to which owner has exclusive rights; IP law is group of laws recognize exclusive rights for creations of mind): **Patents** (to individual or company to protect invention), **trade secrets** (proprietary technical or business info remains confidential, use NDA & encryption), **Trademarks** (symbol, sound, or expression identifying product or org from another org; use capital TM when not registered; R when registered), **Copyrights** (authored work protected from form of reproduction or use without consent of holder; *copyright lasts longer than patent*) WIPO (std copyrights)/CMI (license & ownership)}, **Securing IP**: (Invest in NDA, encryption at storage w/o internet conn, insider threat countermeasures on detection + mitigation); **Corporate info**: plan announcements, process/procedures on profit data/estimates, salaries, market share, perf appraisals;] [**IR process**: *Preparation* (**Training**: [sec awareness training: WHAT, focus on assets must be protected; Security training: HOW, teach personnel skills; Security education: WHY, for security experts as in-house sec programs], Testing, Documentation of procedures; **IR process: Detect / Respond / Report / Recover / Remediate / Review**; Incident form (CMOS); call list/escalation list) -> *Detection & analysis* (***Scope***: 5 factors: **1. downtime/recovery time** [critical (min or hrs)/urgent (<24 hrs)/imp (<72 hrs)/normal (< 7 days)/nonessential (<30 days)] [Max Tolerable downtime: **MTD** OR max period time of disruption: **MPTD**; Mean time to repair: MTTR (single resource or function in a disaster); Mean time b/w failures: **MTBF** (estimated time device will operate before next failure); Recovery time obj (RTO<MTD): **RTO** (shortest time after disaster to restore); Work recovery time (RTO-MTD): **WRT**; Recovery point obj: **RPO**;], **2. data integrity**, **3. economic** [value to owner, costs to maintain, damage if lost, penalties], **4. System process criticality**, **5. reverse engg** (retracing steps in incident as seen from logs in affected devices; **3 ways to make binary readable**: 1. **Disassembly** (reading machine code in memory & o/p each instruction as text); 2. **Decompiling** (reconstruct high-level language source code); 3. **Debugging** (run code interactively; *kernel debugger: ring 0*, *usermode debugger*))) -> *Containment* (**Segmentation**: prevent spread to other segments by limiting scope; layer 2 or layer 3 of OSI; **Isolation** [block all traffic to/from devices by shutdown interfaces; **process isolatio**n: mem dedicated to each process]) -> *Eradication & recovery* (Vuln mitigation: {**Sanitization** (remove traces of threat by overwriting drive many times), Reconstruction/Reimaging, **Secure Disposal** [**clearing** (recoverable w/ forensic tools)**, purging** (sanitization; unreadable w/ adv forensic tools)**, destruction** (degaussing or physical)]}; Patching, Restore perms, Reconstitute resources, restore cap & services, verif of log & comms to monitoring) -> *Post-incident activities* (Evidence retention; **lesson learnt report (LLR)** (1st doc to draft, how/why incident occurred; how to prevent in future; **Qs**: what went right & wrong, how to improve, what needs change, cost of incident); **Change control process** (LLR generate # of changes to n/w infra, follow CC process); IR plan update; **IR summary report** (all staheholders, not too technical, major points: When problem 1st detected/whom, scope of incident, how contained/eradited, work performed during recovery, areas where response was effective, areas to improve); **IoC** (activities that precede/accompany security incident) generation; Monitoring)] |
| PII, **Privacy Impact Assessment (PIA)**, Data classification (security measures for sensitive data types), **Data retention policy** (non-technical control, relies on:datatype, age, legal & regulatory reqs; identifies purpose, org affected, exclusions, personnel responsible for overseeing, data destruction, retention schedule; **Data types**: PII, PHI, PCI; **Legal reqs**: **SOX**: Public Company Accounting Reform & Investor Protection Act of 2002, publicly traded in US; Acct methods/financial report for orgs; penalties/jail time for executives; **HIPPA**: 1996 or **Kennedy-Kassebaum Act**, enforced by OCR (office of civil rights) & HHS (dept of health human services); stds & procedures for storing, using, transmitting medical info/data, amends the Patient Protection & Accordable Care Act (PPACA) or **Obama care**, **GLBA of 1999**: financial institutions, banks, loan companies, insurance, investment, credit card providers, prohibits sharing financial info with 3rd parties, security of PII; **CFAA of 1986**: Computer Fraud & Abuse Act: Hacking of protected computers, 1989, 1994, 1996, 2001 by **USA PATROIT Act**, 2002, 2008 by Identity theft enforcement & restitution act; **Federal privacy act of 1974**: computers w/ records used by fed agency; guidelines on collection, maintenance, dissemination of PII; **Fed Intel Surveillance Act (FISA of 1978)**: law enf & intel agencies, 1st act for physical & electronic surveillance & collection of foreign intel info b/w foreign powers & agents of foreign powers; Amended by USA PATRIOT act of 2001 & FISA of 2008; **ECPA of 1986**: Electronic Comm Privacy Act, Law enf & intel agencies, gov restrictions on wiretaps from phone calls, transmission of electronic data by PC & prohibit access to stored comm., amended by CALEA of 1994 & PATRIOT of 2001, FISA of 2008; **Computer security act of 1987**: Superseded in 2002 by FISMA, 1st law to require formal security plan, protect and defense sensitive info in fed gov systems, gov agencies to train employees & identify sensitive systems; **US Fed Sentencing Guidelines of 1991**: Individuals & orgs convicted of felonies & serious (Class A) misdemeanors; **Comm Assistance for Law Enforcement Act of 1994 (CALEA)**: law enf & intel agencie; telecom carries & manufactures of equipment to modify & design equipment, facility, and service w/ built-in surveillance capabilities; Fed agencies to monitor all phone, internet, VOIP in real time; **PIPEDA: Personal Info Protected & Electronic Doc Act**: private-sector orgs collect, use, disclose personal info in Canada. EU concerns about security of PII in Canada; Obtain consent when they collect, use, or disclosre PII, policies clear, understandable, readily available; **Basel II**: Financial institutions, min capital reqs, supervisory review, market discipline, protect from risks that banks & other financial face; **FISMA of 2002**: Fed Info Security Management Act, Fed agencies, develop, document, implement agencywide infosec program; **Economic espionage act of 1996**: theft of trade secrets (*federal crime*) & individuals using encryption for criminal activities; **USA PATRIOT act of 2001**: Uniting & Strengthening America by Providing Appropriate Tools Req to Intercept & Obstruct Terrorism, law enf & intel agencies, email, telephone records, internet comm, medical & financial records, amended FISA, ECPA of 1986. Doesn’t restrict private citizens use of investigatory tools; **Health care & Education Reconciliation act of 2010**: healthcare & edu org, increased security measures to protect PHI; **Employee privacy issues and expectation of privacy**: emp privacy addressed by all org, protects org from costly legal penalties on data breaches, must give notice of monitoring to employees, must be consistent, *“no-expectation of privacy” policy* (must define unacceptable behavior); **EU:** created Safe harbor principlesto **help US orgs comply with EU privacy ;GDPR**: personal data not processed unless 1 legal basis to do; **Article 6** states lawful purposes: subject given consent, contractual obligations w/ subject, comply with data controller legal obligation, protect subject’s interest, public interest or official, legitimate interests per charter of fundamental rights; **Data sovereignty**: digital data subject to laws of country, where it is located/stored, complicated in cloud solutions, depends on type of data (healthcare and consumer data separate laws), Security prof should answer: Where is data stored, who has access, where is data backup, how is encrypted? **Data Minimization**: lower personal data to store, only necessary, important for GDPR, reduced attack surface; **Purpose limitation**: PII collected for a purpose cannot repurpose without consent; **NDA**: sign if access to trace secrets; | Technical controls: **ACLs, Firewall, Encryption**, **DLP** (integrity & confidentiality), **Data masking** (altering data from original state to protect): substitution, redaction, average, **Data deidentification**: [data anonymization, deleting or masking PII], **Tokenization**: [data hiding/masking, replaces value with token, used in mobile transactions, numeric tokens for cardholders credit/debit card], **Digital rights management (DRM)**: [H/w manuf, publishers, copyright holders, individual use DRM; 1st generation software controls copying; 2nd gen controls executing, viewing, copying, printing, altering; **US Digital Millenium Copyright Act (DMCA) of 1998**: criminal penalties for making tech to circumvent content protection technologies; includes restrictive license agreements & encryption; **Document DRM**: protect confidential/sensitive docs or data; **Music DRM**: subscription-based-service: Napster use DRM to revoke user’s access to downloaded music after subscription expires; **Content Scrambling System (CSS)**: encryption to enforce playback & region restriction on DVD; Hacked using Linux’s **DeCSS** tool; **Advanced Access Content System (AACS)**: Protects Blu-Ray & HD/DVD content; ***DeCSS*** is 1st free program to decrypt content on commercial DVDs; **Video Game DRM**: verify game licenses upon install/allow unrestricted use from that point; **E-Book DRM**: most successful DRM; Kindle, Barnes & Nobles’s Nook devices use DRM to protect electronic form; **ADEPT** (Adobe Digital Experience Protection Technology), uses AES & RSA; **Digital Watermarking**: deter unauthorized use of doc; put logo / trademark / pictures / objects] **Geographic Access Reqs**: Authn systems use **geofencing** (location limits for device usage; uses GPS or RFID for virtual geo boundary); Access Controls. |
| **Robust Risk mgmt**.. **BIA**: how to assess level of criticality of buss function to org; Function analysis, part of BCP/DR; impact of disrupting event on org; *4 steps*: identify critical process/resource, outage impact/estimate downtime, resource req., recovery priority (high,medium,low) | **Risk identify process**: Classification->ownership->Retention->Data types->Retention standards->Confidentiality | **Risk calculation**: probability & magnitude | **Comm of risk factor**: Discuss sharing w/ critical parties | **Risk prioritize**: sec control & engg tradeoff | **Training & exercise**: Red/Blue/White team, tabletop | **Supply chain assess**: vendor due-diligence & h/w source authenticity | **Risk mgmt.**: Formal method of evaluating vuln; **Recoverability**: Ability to recover from disaster event; **Fault Tolerance**: use of backup component, when primary fails; lack of service interruption; backup service ≠ primary service; e.g. high-speed OC1 conn for internet; **Risk identification**: 4 goals: identify assets/value, vuln & threats, probability & impact, balance impact w/ countermeasure; **Formal risk analysis Qs**: 1. What assets to protect, 2. What business needs to org, 3. What outside threats to n/w? [**Qualitative risk analysis**: subjective, uses **risk assessment matrix** (High/Medium/Low on Impact/probability)|intuition, experience, best practice techniques (brainstorm, focus groups, surveys, questionnaire, meetings, interviews, delphi); **Delphi** to estimate likelihood & outcome of future events; 2 advantages: prioritize risk & identify areas of improvement] [**Quantitative risk analysis**: monetary, asset values, threat frequency, vuln severity, impact, safeguard costs; *less guess work*; time & effort to compute & gather info; **SLE = AV x EF**; **ALE = SLE x ARO**;] **Probability** & **Magnitude** is applied to both RA methods (Quantitative: (P) ARO, (M) SLE, Qualitative: (P) event probability, (M) impact); Comm of risk; **Engg Tradeoff**: [**MOU**: Doc (not legal) agreement b/w principals to do something together; **SLA**: service, cost, expectation of perf; **Org gov**: control org activities, process, ops w/o impacting business ops/processes; **Degrading functionality**: creating more issues than resolve; breaks critical apps/process; need alternate soln] **System Assessment**: system vetted for issues from functionality & security. **Certification**: tech system components & **Accreditation**: overall security is accepted by mgmt.; [**ISO/IEC 27001**: 2013 version; obtain cert for info sec; org’s ISMS established, impl, maintain, continually improved; *Components*: ISMS scope, IS policy, RA process, IS personnel competence, IS monitor & measure, Top mgmt. review, Evidence of nonconformities & corrective actions taken; *proj mgr should complete 15 steps*;]; Documented compensating controls; **Red team**: attacking force; pen tests;external **Blue team**: defense; respond to red team attack; practice for real attack; logs, SIEM, Intel, traffic/flow analysis; **White team**: referee b/w red and blue team; enforce rules of engagement; **Tabletop exercise**: cost-effective/efficient to identify vulns; informal brainstorming session; **Vendor due-diligence**: assess vendor’s product/services; **Not purchase counterfeit equipment**: use **OEM** (Original Equipment Manuf) doc; H/w source authenticity, **Trusted Foundry program**: care to ensure authenticity & integrity of h/w components purchased from vendor; DoD identifies trusted vendors/ensure trusted supply chain; 77 vendors; |
| Frameworks: risk-based & prescriptive frameworks; program dev standards, controls, gov methods, process mgmt. methods | **Risk-Based Framework: COBIT**: 2019, **5 domains**: EDM (evaluate, direct, monitor), APO (Align, Plan, Organize), BAI (Build, Acquire, Implement), DSS (Deliver, Service, Support), MEA (Monitor, Evaluate, Assess); [**TOAGF**: 9.2, 2018, Based on: Business Architecture [strategy, gov, org processes], App architecture [apps, relationships], Data architecture [logical, physical], technology architecture [h/w, s/w, n/w infra]; **Architecture Development Method (ADM)** by TOGAF meets business & IT needs of org; (A to H steps)] [**NIST CyberSecurity Framework 2.0**: initially for critical infra; now for all; Govern (Identify, Protect, Detect, Respond, Recover); covers supply chain risk mgmt.] **ISO/IEC 27000 Stds**: (Intl Org for Std, Intl Electrotechnical commission) for BS7799, dev and maintain ISMS; **SABSA**: Sherwood applied buss sec architecture; risk-driven enterprise security arch; 6 comm Qs: What, Where, When, Why, Who, How; [**ITIL**: OMB dev for process mgmt., IT srv mgmt. for aligning ops & srv; 5 pub; ITL service strategy, design, transition, service ops, continual service improve; 26 process; SLAs;] **Maturity Models**: improve process; **CMMI**: guidelines for SDLC; ad-hoc (Initial) to Continuous improve; **Pwd policy** (std word pwd [single words, upper/lower case], combination pwd [composition pwds, mix of dictionary words], static pwd [same for each login, P2P n/w], complex pwd [upper/lower/numbers/special chars], passphrase pwds [long phrase, easy to remember, hard to crack], cognitive pwds [user identity info, questions], OTP [dynamic pwd, highest security, discarded after use], graphical pwds [CAPTCHA], numeric pwds [numbers only]; *pwd life*: duration of valid; *pwd history*: duration before reuse; *Authn period*: duration to remain logged in; *pwd length*: long chars; *pwd complexity*); **Data ownership policy** Data retention; (train people to comply; audit/monitor for compliance; data owner/processors review policy for changes; security professionals ensure security is considered & policy satisfies org needs) Account mgmt (elements of acct mgmt.: 1. Establish formal process for create/close acct, 2. Review user acct, 3. Track access authz, 4. Rescreen In sensitive positions, 5. Verify legitimacy of user accts) (mgmt. of IDs & Accts, access control provisioning lifecycle); Continuous Monitoring tool w/ baseline: **SCT (Sec Compliance Toolkit**), Group Policy, MESCM; Work Product Retention (o/p belongs to org); **Controls** types: **Managerial**/Administrative/Soft | **Operational** (*Directive* [acceptable practice in org, AUP, effective only when consequence is stated for not-following directions], *Deterrent*: triggers prevent & corrective cntrls) | **Technical**/Logical; **Control mechanisms**: Preventative, Detective, Corrective, Deterrent, Directive, Physical, Audits & Assessment, **Regulatory** (2011, Stmt on Stds for attestation engagements, SSAE,No. 16 replaced SAS70, for auditing service orgs, now updated to v18; verify controls/process in place by data-center are followed; SSAE 18 also require written assertion reg design & operating effectiveness of controls being reviewed) (**SOC1** financial report **type 1**: [auditor opinion of accuracy of DC design/control/service], **SOC1 type 2** [type1 + over period of time, 6 to 12m], **SOC2** security, CIA, privacy [service auditor test & results; clients/regulators/stakeholders], SOC3 [soc2 but general public]), Compliance; |

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act)