AGENCY REQUIRED POLICY CHECKLIST

□ Relationship to Local Security Policy and Other Policies - CSP Section 1.3

"The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy, and, where applicable, the local security policy."

- Does the agency have a policy that states the agency must comply with the CSP?
- Does the agency have documented procedures to facilitate the implementation of the CSP?

□ Personally Identifiable Information (PII) - CSP Section 4.3

"Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from criminal justice information (CJI)."

- Does the agency have a Personally Identifiable Information policy?
- Does the policy describe appropriate security controls for handling PII extracted from CJI?
  - Physical protection
  - Logical protection
  - Dissemination

□ Information Exchange - CSP Section 5.1.1

"In these instances, the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate the requestor of CJI as an authorized recipient before disseminating CJI."

- Does the agency have a policy stating how agency members will validate the requestor of CJI is an authorized recipient before disseminating CJI?

□ Information Handling - CSP Section 5.1.1.1

"Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration, or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange."

- What are the agency's procedures for handling, processing, storing, and communication of CJI?
- Do the procedures provide criteria for how personnel are to protect information from unauthorized disclosure, alteration, or misuse?

□ Incident Response - CSP Section 5.3

"Agencies shall (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities."

- Does the agency have a policy that describes how the agency prepares/has prepared for a security incident?
- Does the policy describe how the agency detects, analyzes, contains, and recovers from a security incident?
- Does the policy describe actions the user should take in the event of a security incident?
- Does the policy describe how agency personnel track, document and report the incident to the appropriate agency officials and the FDLE Information Security Officer?
- The policy should include physical and electronic incident response.

□ Incident Response - CSP Section 5.13.5

"In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address <u>mobile device</u> operating scenarios."

- Does the policy include additional reporting and handling procedures for mobile devices?
    - Loss of device control
    - Total loss of device
    - Device compromise
    - Device loss or compromise outside the United States
- Agency can combine in incident response plan for the agency.

□ Account Management – CSP Section 5.5.1

"The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process."

- Does the policy describe how the agency manages information system accounts, including:
  - Establishing,
  - Activating,
  - Modifying,
  - Reviewing,
  - Disabling,
  - Removing accounts?
- Does the policy describe how often the agency validates the information system accounts (at least annually)? If more than annually, how often?

□ System Access Control - CSP Section 5.5.2.2(1)

"Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions."

- Does your policy prohibit multiple concurrent active sessions?
- If not, does your policy describe the operational business needs of allowing multiple concurrent sessions?

□ Remote Access - CSP Section 5.5.6

"The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system."

- Does the agency policy describe the technical process for enabling remote access?
- Does the agency policy describe the administrative process for enabling remote access?

□ Personally Owned Information Systems - CSP Sections 5.5.6.1

"A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices."

- Does your policy prohibit the use of personally owned information system from accessing, processing, storing, and/or transmitting CJI?

□ Authentication Strategy - CSP Section 5.6.2

"The authentication strategy shall be part of the agency's audit for policy compliance."

- Does your policy describe the implementation requirements of all the authentication strategies used?
  - Password requirements (CSP password requirements)
  - Advanced Authentication

□ Authenticator Management - CSP Section 5.6.3.2(2)

"Agencies shall establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators."

- Does your policy describe the procedure for initial authenticator distribution?
- Does your policy describe the procedures for lost/compromised authenticators?
- Does your policy describe the procedure for repair/reissue damaged authenticators?
- Does your policy describe the procedure for revoking authenticators (voluntary/involuntary)?

□ Media Protection - CSP Section 5.8

"Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media."

- Does your policy describe procedures to ensure access to electronic and physical media is restricted to authorized individuals?
- Does your policy include procedures to ensure secure:
  - Handling media?
  - Transporting media?
  - Storing media?

□ Electronic Media Sanitization and Disposal - CSP Section 5.8.3

"The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel."

- Does your policy describe the steps your agency takes to sanitize or destroy electronic media?
- Does your policy state the sanitization or destruction will be witnessed or carried out by authorized personnel?

□ Disposal of Physical Media - CSP Section 5.8.4

"Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."

- Does your policy describe the procedures to securely dispose of physical media?
- Does your policy state the disposal or destruction of physical media will be witnessed or carried out by authorized personnel?

□ Physical Protection - CSP Section 5.9

"Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures."

- Does your policy describe how CJI is protected through access control measures?
  - Include access control measures for information system hardware, software, and media (electronic and physical)?

□ Encryption - CSP Section 5.10.1.2.3

"For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system."

- Does your agency use public key infrastructure to access CJI? If not, your agency should state so.
- If your agency uses public key infrastructure, does your policy describe how the certificates are issued to agency personnel?

□ Voice over Internet Protocol - CSP Section 5.10.1.4(1)

When an agency deploys VoIP within a network that contains unencrypted CJI, the following additional control shall be implemented: "Establish usage restrictions and implementation guidance for VoIP technologies."

- Does your agency use VoIP on the network containing CJI? If not, your agency should state so.
- If your agency uses VoIP, does your policy describe the agency usage restrictions?
- If your agency uses VoIP, does your policy describe how VoIP will be implemented on your agency's network?

□ Patch Management - CSP Section 5.10.4.1

"The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as: 1. Testing of appropriate patches before installation. 2. Rollback capabilities when installing patches, updates, etc. 3. Automatic updates without individual user intervention. 4. Centralized patch management."

- Does your policy describe how patches are promptly installed for newly released security relevant patches, service packs, and hot fixes?
- Included should be how the agency conducts:
  - Testing of appropriate patches before installation.
  - Rollback capabilities when installing patches, updates, etc.
  - Automatic updates without individual user intervention.
  - Centralized patch management.

□ Security Alerts and Advisories - CSP Section 5.10.4.4

"The agency shall document the types of actions to be taken in response to security alerts/advisories."

- Does the agency policy describe how the agency:
  - Receives information system security alerts/advisories on a regular basis.
  - Issues alerts/advisories to appropriate personnel.
  - Documents the types of actions to be taken in response to security alerts/advisories.
  - Takes appropriate actions in response.
  - Employs automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

□ Personnel Sanctions - CSP Section 5.12.4

"The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures."

- Does your policy describe the sanction process for personnel that fail to comply with established agency policies and procedures?

□ Wireless Access Restrictions - CSP Section 5.13

"Agencies shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system."

- Does your agency use wireless access for CJI (laptop, MiFi, wireless access points, mobile hotspot, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR)? If not, your agency should state so.
- If your agency uses wireless, does your policy describe
  - Usage restrictions for all mobile devices?
  - How your agency will authorize, monitor, and control wireless access to the information system?

□ Review of Wi-Fi Logs - CSP Section 5.13.1.1(14)

"Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly."

- Does your agency policy describe how often logging will be reviewed (must be at least monthly)? If more than monthly, how often?

□ Bluetooth - CSP Section 5.13.1.3

"Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency's operational and business processes."

- Does your agency use Bluetooth (cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices) for connect to a device accessing CJI? If not, your agency should state so.
- Does your agency policy describe the use of the Bluetooth and its associated devices?