Implementation Frequently Asked Questions

Implementation questions:

1. **Are there instances when both the Secure Software Configuration Standard and the Secure Development Standard would apply?**

Yes. For example, in the case of a purchased application that a Unit customizes by developing or adding software to meet the needs of the user, the Secure Software Configuration Standard would apply to the purchased elements and the Secure Software Development Standard would apply to the elements developed by UC.

Another example would be when the Unit has developed an application, but purchased some component, like a report writer, to meet the user's needs. In this case, the Secure Software Development Standard would apply to elements developed by UC and the Secure Software Configuration Standard would apply to the report writer.

2. **Should the Encryption Key and Certificate Management Standard be used as a source of requirements for API keys?**

Yes. An API key can be treated like other secret security keys. All cryptographic keys that provide confidentiality or integrity functions and rely on secrecy should be protected as P4.

3. **When data elements are added or the data architecture changes, could there be an impact to the classification of Institutional Information?**

Yes. As an example, consider a report that characterizes visits to the Dean of Students Office. If the report identifies the reason for the visit by broad category, a classification of P1 or P2 may be appropriate. However, if a data element is added, such as day and time of visit, then it could potentially impact the privacy of individuals visiting the Dean of Students. In this case, the report would require a higher Protection Level.

4. **In the Secure Software Development Standard, could Section 4.12 Secure Configuration include a web application scan?**

Yes. The requirement is to perform a vulnerability scan of the entire solution. This should be interpreted broadly and include all scans or analyses needed to ensure the solution is secure. These scans could cover unaddressed vulnerabilities, coding syntax, vulnerabilities, logic fuzzing, and other application weaknesses.

5. **In the Event Logging Standard, does Section 4.1's requirement for the logging plan to identify "Log access controls" include both authentication and authorization?**

Yes. The requirement is to determine both which roles have access to the logs and how that access is granted.