OMB Control No. 0693-0043

Expiration Date: 12-31-2018

Usable Cryptography - Interview Questions

1. Without using your organization's name, can you please tell me about your organization – what it does, what it produces?

2. What is your role within your organization with respect to cryptographic products?

3. How did you get into software development?

   - At what point and why did you become concerned with cryptography and secure development?

4. Do you work in a unit or department that is part of a larger organization?

   - [If yes]: What is the size of the unit or department?
   - What is the size of your overall organization?

5. Can you tell me about the kinds of products your organization develops, and specifically those that use cryptography?

6. Who are the target customers for your products that use cryptography?

7. How long has your organization been working on products that use cryptography?

8. Can you tell me about the importance of cryptography within your organization? For example, is it your primary business focus, or is it an enabler within your products?

9. For your products that use cryptography, what processes or techniques does your organization use to minimize bugs and errors in code during the development process?

    - What formal policies does your organization have for secure product development?

10. What processes or techniques does your organization use to test and validate the cryptography component in your products?
    - What formal policies does your organization have for secure product testing?

11. Why does your organization choose to use these methods? (for example, industry standard, customer demand, robustness and quality)?

    [Probe on each individual reason, for example, if customer demand/requirements are a reason:]

    - What are your customer requirements regarding testing? How do these requirements add value to your products, if at all?

    [If third party testing was mentioned in the answer to the previous question]

    - What reasons led you to decide to use third-party testing?
    - How do you establish confidence in the results of the third-party testing?

12. What, if any, are your organization's biggest challenges with respect to testing cryptography within your products?

    - How do you think these challenges can be overcome, if at all?

13. What references do you use to help you create test plans for the cryptography component of your products? (for example, standards, industry specifications, books, academic papers)

    [If the participant does NOT use standards]:

    - Why doesn't your organization use standards?

[If the participant uses standards:]

14. For what reason(s) does your organization choose to use standards?

15. How do you use standards when you create a test plan?

16. What kinds of standards do you use?

17. What do you see as the value or benefit of using these standards, if any?

[For all:]

18. How could standards or other testing guidance be improved to make testing easier, if at all?

19. Updates or changes to crypto algorithms, standards, and libraries can be more gradual and expected, for example a refresh or deprecation of an algorithm or a move to a more robust standard, or they may be more time-sensitive and unexpected, for example patching a vulnerability in a crypto library. We're going to address both cases separately.

    - First, let's consider time-sensitive issues, for example vulnerability-related updates. How, if at all, do you modify your typical testing process or methods to address these?

    - How do *non-vulnerability* updates or changes to cryptography algorithms and standards affect your testing process or methods, if at all?

20. Is there anything else you'd like to add about the topics we've discussed?