Usable Cryptography - Interview Questions

1. Can you 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 this field?

    - At what point and why did you become concerned with cryptography and secure development?
    - In which field(s) is your formal education?

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 typical customers for your products that use cryptography?

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

8. Is cryptography your organization's primary business focus, or is it an enabler within your products?

9. For your products that use cryptography, what processes or techniques , if any, does your organization use to minimize bugs and errors in code during the development process?
    - Why does your organization choose to use these methods? *[only use if participant has difficulty coming up with response:]* for example, industry standard, customer demand, robustness and quality

10. What processes or techniques does your organization use to test and validate the cryptography component in your products?
    - Why does your organization choose to use these methods? *[only use if participant has difficulty coming up with response:]* for example, industry standard, customer demand, robustness and quality
    - What kind of end-user testing, if any, does your organization do to prevent customers from misconfiguring or misusing the cryptography component in your products?

11. Does your organization do any certifications or third party testing?
    - What reasons led you to decide to use certifications or third-party testing?
    - How do you establish confidence in the results of the certifications or third-party testing?
    - What are the challenges or issues your organization has experienced with certifications or third-party testing, if any?

12. What, if any, are your organization's biggest challenges with respect to developing and testing cryptography within your products?
    - How do you think these challenges can be overcome, if at all?
    - Has your organization experienced a tension between secure development and testing and getting a product to market? If so, how has that impacted your organization's processes?

13. Do your customers have specific requirements regarding development and testing? If so, what are those requirements?

14. How do updates impact your development and testing processes, if at all? *(time-sensitive vs. deprecation)*

15. What resources do you use to help you develop and test the cryptography component of your products? *[only use if participant has difficulty coming up with response:]* for example, standards, industry specifications, books, academic papers, standard libraries, APIs
    - What are the reasons your organization chooses to use those particular resources?

    [If the participant does NOT use standards]:
    - What are the reasons that your organization does not use standards?

16. [If the participant uses standards:] What kinds of standards do you use?
    - What is the role of standards in your organization's development and testing processes?
    - What do you see as the value or benefit of using these standards, if any?

17. How could standards or other cryptographic resources be improved to be more useful?
    - How could NIST standards and guidance be improved to be more useful?

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

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 60 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Mary Theofanos, maryt@nist.gov, (301) 975-5889.

OMB Control No. 0693-0043

Expiration Date: 12-31-2018