Questions to [Carrier] on Mobile Device Security

In responding to these questions, we ask that [Carrier] supplement its qualitative descriptions with supporting data about security updates and customer devices. Additionally, where any answers regarding practices or policies responsive to the questions below differ for any wholly-owned mobile virtual network operator, please describe how those practices or policies differ.

General Questions

1. Does [Carrier] face issues or hurdles in releasing security updates for operating systems (OS) to consumers? If so, please explain in detail.
2. Do any mobile devices on [Carrier]'s network run an OS that is modified for or is unique to [Carrier] and if so, what percent of the devices on [Carrier]'s network do they represent? With respect to such OS, is [Carrier] responsible for developing and providing security updates? Does [Carrier] face any additional issues or hurdles in releasing security updates for such OS to consumers? If so please explain in detail.
3. Similarly, are there devices intended for deployment on [Carrier]'s network that have been loaded at [Carrier]'s direction with special software beyond the OS or applications to monitor device or network performance or similar metrics (Required Software)? With respect to such Required Software, is [Carrier] responsible for developing and providing security updates? Does [Carrier] face issues or hurdles in releasing security updates for Required Software to consumers, regardless of who is responsible for developing such updates?
4. Does [Carrier] face particular issues or hurdles in getting consumers to install updates for either a modified OS or Required Software on mobile devices as they are made available?
5. To what degree does [Carrier] know whether a consumer has installed a security update to address OS or Required Software security vulnerabilities? If [Carrier] does not engage in practices to monitor such information, does [Carrier] have the technical ability to do so?
6. To the extent that [Carrier] does not know whether individual consumers have installed updates to address security vulnerabilities in an OS or Required Software, is [Carrier] concerned about this lack of knowledge?
7. Could unpatched, non-updated devices on [Carrier]'s network impact or harm the functionality of that network or [Carrier]'s ability to provide effective service to other consumers who have patched and installed security updates on their devices?

Development and Release of Security Updates Questions

8. To [Carrier]'s knowledge, what entities are involved in the updating process (e.g., original equipment manufacturer (OEM), OS or Required Software vendor, other) and can any of those entities other than [Carrier] individually release security updates for the consumer directly? What legal, security, or other permissions are required from any involved entities and does obtaining those permissions cause delay in release? If [Carrier] provides updates to consumers, are security updates generally released to all consumers at once? If not, please describe the security update release process and how it might affect different consumers, including those who transfer their device to [Carrier]'s network.
9. Do any of these answers differ for devices running different operating systems (e.g., Android, Windows, iOS, CyanogenMod, Blackberry, etc.)? If so, describe in detail. Is the process different for devices that are ported to [Carrier]'s network? If so, describe in detail.

10. As a general matter, are security updates that have been made available or provided to [Carrier] by an OEM or OS or Required Software vendor in response to an identified security vulnerability regularly reviewed and/or released by [Carrier]? If so, how long does this process take? If not, please explain.

11. What considerations does [Carrier] generally take into account when determining the prioritization and timing of release of a security update (i.e., severity of vulnerability, whether it can be rolled into another planned update, etc.)?

12. What data does [Carrier] maintain about security updates that have been made available to [Carrier] and the actions [Carrier] has taken in response?

Consumer-specific Questions

13. Does [Carrier] provide updates to consumers with vulnerabilities on their mobile devices or make available a website where consumers can easily check the vulnerability status of their device and download required patches? If so, what are the steps and typical time frames from the discovery of a vulnerability to the consumer receiving an update that resolves the vulnerability—or making that vulnerability available for download?

14. Are there instances where [Carrier] knows of a vulnerability to OS or Required Software but does not release a security update to consumers or otherwise make the security update available? If so, why and how does [Carrier] protect consumer security in such instances?

15. Does [Carrier] discontinue security update support for mobile devices? How does [Carrier] decide when to discontinue security update support? Are consumers notified at the time of sale how long security updates will be provided or supported for their device by [Carrier]? Are consumers notified when security updates to their mobile devices are no longer supported? What are consumers' options for protecting themselves against security vulnerabilities after such discontinuance by [Carrier]?

16. What information or notices regarding security update support does [Carrier] provide to customers who port or bring their device when they sign up for [Carrier]'s service?

Stagefright-specific Questions

17. When and how did [Carrier] first become aware of vulnerabilities in the Android libstagefright library (commonly known as Stagefright)?

18. How many models of mobile devices on [Carrier]'s network were or might/could have been impacted by Stagefright vulnerabilities?

19. How many models of mobile devices on [Carrier]'s network remain vulnerable to the Stagefright vulnerabilities? Approximately how many such devices remain active on the network? How many of these devices have a customized OS provided by the [Carrier]?

20. Following expressions of public concern surrounding the Stagefright vulnerabilities, Google, Samsung, and LG committed to releasing monthly security updates for mobile devices. Has [Carrier] made a similar commitment to expedite the release of the monthly security updates as they become available? Have such monthly updates been made available and, if so, has [Carrier] begun to release those updates as they become available? How many have been made available and how many has [Carrier] released?