DECEMBER 2016

LEVERAGING COMMERCIAL TECHNOLOGY

Early Adoption of Emerging Mobility in the Pentagon

Ben FitzGerald and Alexandra Sander

Center for a New American Security

About the Authors

BEN FITZGERALD is the Director of the Technology and National Security Program at the Center for a New American Security. His work focuses on the intersection of strategy, technology, and business as they relate to national security. Recent projects have included analysis of the future of the global defense industry, U.S. military technology superiority strategies, cyber security collaboration, and innovation within the Department of Defense. Prior to CNAS, FitzGerald founded the U.S. subsidiary of an Australian strategy firm, Noetic, leading their work with the Pentagon, military services, and the U.N. Earlier in his career, he worked with information technology companies IBM, Rational Software, and Unisys. His work and commentary have been featured in the media from C-SPAN to Vice

ALEXANDRA SANDER is a research associate with the Technology and National Security Program at CNAS. Previously, she was a research assistant with the NATO Parliamentary Assembly in Brussels, Belgium. There, she primarily supported the Science and Technology Committee's research and reporting on the global spread of ballistic missile defense systems and Euro-Atlantic cybersecurity policy. Ms. Sander holds a B.A. in political science from California Polytechnic State University San Luis Obispo and an M.A. in international security from the University of Denver's Josef Korbel School of International Studies.

About Future Foundry

The Future Foundry project seeks to develop and articulate a positive, 21st-century vision for sustainable collaboration between the Department of Defense and its partners from multiple industry sectors. The project builds on two years of research by the CNAS team describing the challenges faced by the global defense industry in "Creative Disruption" and considering DoD's attempts to maintain military-technical superiority in "Beyond Offset." Now, with widespread recognition that the existing defense industrial regime is optimized to cope with neither the rapidly evolving and varied threat landscape nor the decentralization of innovation and global proliferation of advanced technology, there is an opportunity to initiate meaningful change.

Acknowledgements

We would like to thank our colleagues at CNAS for their support of the project and their critical feedback on the report. In particular, we are grateful to Michèle Flournoy for her substantive advice, to Shawn Brimley for his editorial guidance, and to Melody Cook and JaRel Clay for their publication and media assistance.

Readers should note that some of the steering committee and working group participants are affiliated with organizations that support CNAS financially. CNAS maintains a broad and diverse group of more than 100 funders including private foundations, government agencies, corporations, and private individuals, and retains sole editorial control over its ideas, projects, and products. A complete list of our financial supports can be found on our website.

The views expressed in this report are those of the authors alone, who are solely responsible for any error of fact, analysis, or omission.

Cover Photo Credit
iStock Photo

Introduction

Rapid advances in mobile computing offer the Department of Defense significant benefits. Leveraging the capabilities of leading-edge mobile devices within DoD could amplify the positive impact of workforce mobility, enhance information security, and instigate the modernization of aging information technology infrastructure within the Pentagon.[1] Yet the department's risk-averse culture and intractable acquisition policies likely will cause it to squander these opportunities in favor of outdated, more expensive, and less effective mobility solutions.

Commercial mobile devices are putting more computing power in the hands of consumers than ever before, delivering impressive capabilities at higher performance levels. Increasing processor speeds and more efficient power consumption – alongside expanding data storage options, widening global spectrum availability, and the proliferation of more sophisticated sensors – are narrowing the gap between what is achievable on a mobile device and tasks that require a personal computer.[2] In the next few years, not only will handsets and tablets be able to do more, but they also will offer increasingly robust security measures, reaching new levels of physical and data security.[3]

Early adoption of this next generation of mobile devices would allow the Department of Defense to improve information technology outcomes in the Pentagon and, further, reclaim the role it played as a technology leader decades ago, investing in nascent internet and global positioning system technologies. Embracing leading-edge mobility will revitalize workforce mobility, modernize information systems, and send a demand signal to suppliers that will shape future commercial roadmaps in key technology areas with benefits that extend to the warfighter, such as machine learning and sensor development.[4]

To take this step, DoD will have to overhaul its existing mobile policies and take a new approach to device procurement. Although some groups within the department, including the Office of the Chief Information Officer, are experimenting with new models of mobility, many of the devices issued to employees are years behind what is commercially available and their performance is hindered by restrictive security measures.[5] It is telling that BlackBerry, the preferred handset manufacturer among highly regulated industries, including DoD, is struggling to keep up with its competitors in almost every other marketplace and is attempting to offset poor device sales by expanding the software and services side of their business.[6] If DoD continues to lag behind the commercial curve, they will spend more to maintain outdated technology that delivers inferior security and business outcomes.

In the next few years, not only will handsets and tablets be able to do more, but they also will offer increasingly robust security measures, reaching new levels of physical and data security.

Slow to Adopt and Slow to Adapt

The department's reliance on old information technology, even when new and better options are available, is a consequence of applying inflexible, drawn-out procurement policies skeptical of commercial off-the-shelf (COTS) products to a field of technology that advances and evolves rapidly. In an effort to limit risk, assumptions about how mobile devices impact the security of DoD information systems end up embedded in policy. As a result, aging policies favor the preservation of familiar but outdated technologies and information security techniques over modernization because they more accurately match the requirements identified at the time the policy was developed.

At the core of workforce mobility is improved connectivity to corporate data through small form factor devices: handsets and tablets. The extent to which businesses and organizations take advantage of mobility depends both on the security of the devices in use – including everything from hardware to applications downloaded from the internet – and the level of risk to corporate data those organizations are willing to assume.[7] Until recently, mobile devices were significantly less secure than their larger form factor counterparts (desktop and laptop computers), lacking the physical space, power, and energy to support comparable security features. Consequently, integrating mobile devices into heavily regulated industries has often required a trade-off that prioritizes security through strict control over device capabilities and use cases at the cost of the user experience.

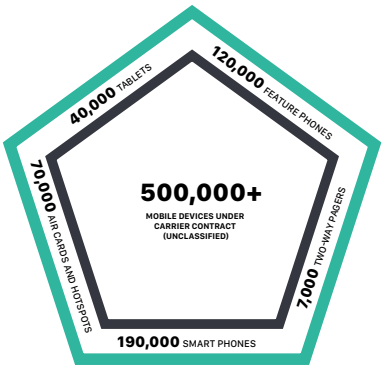
The assumption that mobile devices inherently pose a higher degree of risk to the networks and information they have access to underpins the procurement method and model of workforce mobility the Department of Defense employs today. Because COTS devices are perceived to be insecure, DoD only procures mobile devices that are certified as in compliance with the Committee on National Security Systems Policy governing information technology acquisition and are configured according to DoD Security Technical Implementation Guides.[8] These devices are then issued to employees according to a corporate-owned business-only (COBO) model that prohibits personal use of DoD handsets.

Strict guidelines managing workforce mobility allow the department to control what devices are capable of at the hardware and software levels and how they are used, such as by disabling cameras and Bluetooth transmissions and managing access to downloadable applications. While this approach may help minimize some risks of exposing DoD information systems and data to malicious actors, it also turns highly capable pieces of technology into devices that can perform only a few useful tasks – namely, to send and receive email.

Letting outdated policies drive mobile technology strategies will ultimately undermine the security of DoD information systems as opportunities to take advantage of new capabilities are left unexplored and employees, looking to replicate the modern user experience achievable on their personal devices, start to work around the system.[9] Instead, DoD should endeavor to be an early adopter, letting advanced mobile technology inspire new use cases and applying policy to guide efficient adaption and address gaps in security when necessary.

Aging policies favor the preservation of familiar but outdated technologies and information security techniques over modernization because they more accurately match the requirements identified at the time the policy was developed.

Snapshot of the DoD's Mobility Program



DoD Mobility Unclassified Capability

Allows government purchased commercial mobile devices access to:

- Department of Defense Information Network
- Defense Enterprise Email, calendar, contracts, tasks, and notes
- Encrypted email capability
- Approved applications

DoD Mobility Classified Capability

Allows Defense Information Systems Agency provided, NSA approved mobile devices access to:

- Secret Internet Protocol Router Network
- Domestic and international service
- Secure Voice over Internet Protocol
- Secure Outlook Web Access

Multi-vendor Approach

- **Mobile devices** are purchased from vendors that participate in the National Information Assurance Partnership and demonstrate compliance with the applicable technology protection profile. Vendors include Samsung, Microsoft, Apple, LG, Boeing, and BlackBerry.
- **Operating systems** in use are developed by vendors including Apple, Android, and Windows.
- **Cell phone** carriers contracted include Apple, Android, and Windows.

Data from 2015 derived from the DoD CIO Mobility Industry Day Mobility Update/Overview (July 9, 2015).[19]

An Alternative Model

Deploying leading-edge mobile technology will not only modernize DoD workforce mobility, but also will enable broader applications of mobile computing power that can improve productivity, efficiency, and information security. However, the extent to which DoD will experience the benefits of next-generation mobility will depend heavily on the revision of outdated mobile procurement policies and models of workforce mobility.

The Technology

In the next two to four years, commercial mobile devices will have the right combination of hardware and computing power to drastically reduce the vulnerabilities typically associated with mobility – from limiting the impact of poor user behavior to protecting sensitive data from malicious actors. The confluence of technological advances in a few core areas will allow the next generations of handsets and tablets to offer a host of features that, when combined, will vastly improve information security. With this new baseline for device security, DoD will be able to leverage the full suite of capabilities available on next-generation mobile devices while modernizing workforce mobility and information technology infrastructure.

In particular, the combination of the following capabilities, some of which are already offered on commercial mobile devices, will provide the foundation for the expansive adoption of leading-edge mobile devices within DoD.

CONTINUOUS MULTI-FACTOR AUTHENTICATION

Today's smartphones are already leaving behind the notoriously insecure password, offering biometric verification options (retinal and fingerprint scans) as sign-on credentials and allowing users to adjust verification settings based on their location.[10] In the near future, powerful processors and more capable sensors will enable mobile devices to conduct continuous, multi-factor authentication via the verification of multiple biometric signatures and patterns of behavior, such as keystroke dynamics. Instead of prompting users to provide credentials at pre-determined intervals, handsets and tablets will constantly verify users' identities, increasing the physical security of mobile devices and the difficulty of stealing or faking credentials to gain access to data.

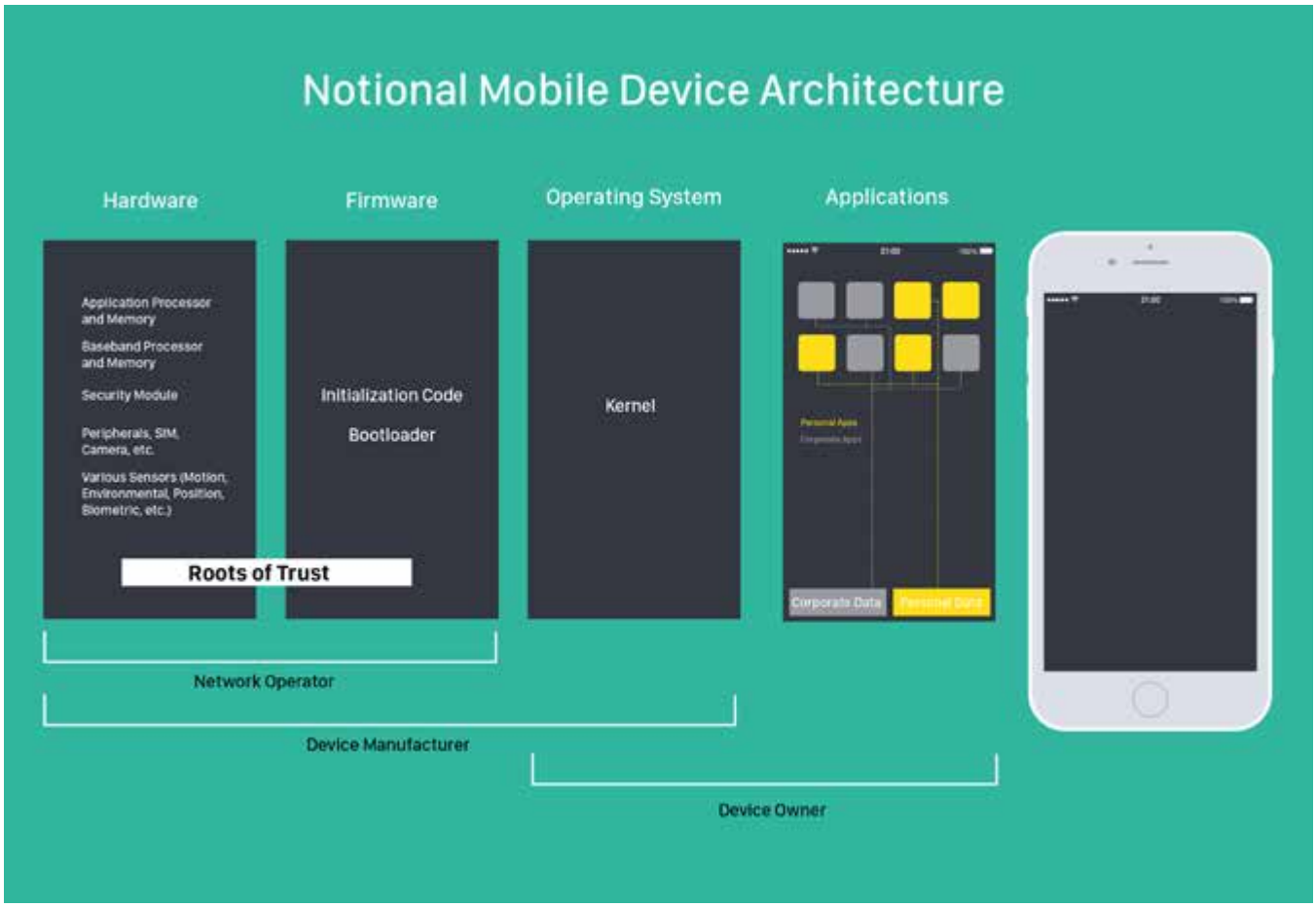
DEVICE INTEGRITY AND DATA SECURITY

Hardware-based security and methods of protecting and isolating sensitive data can provide new levels of assurance that devices' hardware, firmware, and software have not been corrupted and their operation will not compromise information security. In the same way user authentication verifies a trusted device operator, so-called "roots of trust" embedded inside hardware components, where they are most secure, are a foundational security element that provides evidence and verification of device integrity and ensures that a handset or tablet is operating as authorized.[11] Furthermore, while devices are running in a trusted state, sensitive data can be isolated to prevent interaction with less secure software or applications running on a mobile device and vice versa. Methods of isolation such as session management, virtualization, and sandboxing offer varying degrees of separation, from creating isolated environments within an operating system to setting hardware level boundaries.

SECURE NETWORK ACCESS AND SIGNATURE MANAGEMENT

While the physical security of mobile devices and data-at-rest is essential, it must be complemented by equally trusted methods of remotely accessing and transporting data in order for mobility to be both secure and useful. Virtual private network (VPN) tunneling allows for secure communications across public networks by encrypting and encapsulating packets of data.[12] Mobile use of VPN tunnels allows devices to securely and remotely connect to private networks. Data-in-transit can be further protected by hardware that maximizes signature management strategies. Multiple input/multiple output methods of transmitting data allow mobile devices to send and receive packets of data that have been broken up and sent from multiple antennas. What this means is that single streams of data contain incomplete information, reducing the risks posed by interception.

Combined, these features maximize the security of data-at-rest and data-in-transit while supporting superior performance and a satisfying user experience. Leveraging the full spectrum of capabilities of near future mobile devices would not only push DoD to the forefront of workforce mobility but also would increase



This graphic is derived from the National Institute of Standards and Technology report, Guidelines on Hardware-Rooted Security in Mobile Devices. It describes a notional mobile device architecture stack of hardware, firmware, and software.[20]

the security and business value of existing information technology infrastructure. In particular, applying the higher, more accurate standards of authentication provided by advanced mobile devices to public key infrastructure within the Pentagon could significantly improve information security simply through better access control.

In Practice

When businesses and organizations put mobile devices to work, they consistently experience increased productivity and improved efficiency.[13] More flexible and secure access to DoD data will certainly compound the common benefits of workforce mobility, but leading-edge mobile technology can provide even more advantages unique to the DoD use case.

INCREASED PRODUCTIVITY AND IMPROVED EFFICIENCY IN CLASSIFIED SETTINGS

Currently, secure remote access to classified networks and data among cleared DoD employees exists only at the Secret level on select government and commercial devices separate from the unclassified portfolio.[14] Furthermore, the use of mobile devices is prohibited within sensitive compartmented information facilities, often preventing employees with offices in a classified space from taking advantage of capabilities unique to mobile devices during working hours. Expanding employees' classified mobility and access to data could dramatically increase productivity and improve efficiency because the current baseline of classified mobile services is so low. Supporting efficient collaboration at classified levels via enhanced mobility is essential among a workforce that is dispersed within a large building with complex and restrictive access procedures and between employees on frequent and extended travel.

U.S. Army General Martin E. Dempsey discusses cybersecurity at a June 2013 Brookings Institution conference, speaking positively of network consolidation efforts and 4G wireless access for certified smartphones and tablets. (D. Myles Cullen/DVIDS)

INFRASTRUCTURE BENEFITS

The authentication credentials and security of next-generation mobile devices offer the Department of Defense an opportunity to re-evaluate the role of its aging information technology infrastructure and initiate necessary modernization efforts. Beyond security, commercial mobile devices offer a host of capabilities that could replace duplicative, single-function systems throughout the Pentagon with more effective solutions that will lower long-term costs:

- Replacing identification and public key infrastructure credentials with the continuous, multi-factor authentication provided by mobile devices offers a more secure alternative to the common access card (CAC). While requiring an upfront investment, eliminating CAC cards and readers eventually would reduce IT maintenance costs as modernization would effectively occur alongside mobile device updates.
- Mobile authentication methods combined with complete desktop virtualization would allow DoD to remove hard drive storage from personal computers, centralizing sensitive data on department servers or with cloud services. This approach would support a work environment in which employees can transition seamlessly between devices and maximize productivity wherever they work.
- Conducting videoconferences over mobile devices would allow the department to eliminate the need to use and maintain Tandberg systems, allowing interagency partners with lower IT budgets to collaborate with DoD without purchasing expensive videoconferencing equipment.

Bring Your Own Device to the Pentagon

The Department of Defense could acquire leading-edge mobile devices through the current COBO model, but in order to capitalize on all the benefits advanced mobility has to offer and continue to stay current as the technology progresses, DoD instead should take a bring your own device (BYOD) approach. Allowing DoD employees to use their personal devices for work would be cheaper, easier to manage, and lead to better technology outcomes.[15] Furthermore, implementing the BYOD model would not require large procurement efforts, simply a revision of policy, making this new approach an easy but unlikely solution for the department.

The BYOD approach is not without federal

support – as early as 2012, the federal chief information officer issued a toolkit supporting agencies seeking to implement a BYOD model of mobility.[16] In a 2013 memorandum on Department of Defense Commercial Mobile Device Implementation Plan, the department identified BYOD as a "long-term objective," but noted that "existing DoD policies, operational constructs, and security vulnerabilities currently prevent the adoption of devices that are unapproved and procured outside of official government acquisition."[17] With advanced mobile technology's significant improvements to device security, the major barriers to adoption are within DoD's control.

A BYOD model would require DoD to do little beyond establish minimum requirements for mobile devices, develop a provisioning mechanism to configure personal handsets and tablets, and install more robust wireless infrastructure, such as base stations and repeaters. While this transition will incur some added costs at the outset, the long-term benefits of BYOD are significant.

BENEFITS

First and foremost, a BYOD model of mobility would eliminate many future obstacles to adopting the next generations of leading-edge mobile technology. Allowing employees to use their personal devices for work will increase the speed of device turnover and introduce a wider variety of mobile devices at DoD. As a result, DoD will naturally implement device upgrades as mobile technology continues to improve, experiencing more immediate benefits from commercial competition as different manufacturers rise and fall. Policy that is adaptive to incremental changes in technology will better prepare the department for broad future trends, such as the move away from cabled information systems to wireless infrastructure.

Second, given the ubiquity of highly capable commercial devices, BYOD would eliminate the gap between the user experience employees are able to achieve on their personal handset or tablet compared to their DoD devices under a COBO model. Employee satisfaction would rise, as BYOD offers a more modern and customizable user experience and streamlines personal and work computing on a single, dual-use device. Reducing DoD users' frustrations would also curb attempts to work around limited models of workforce mobility, lowering the risks to information systems introduced by unauthorized user behavior.

Third, implementing the BYOD approach would be less costly than attempting to recreate its benefits via alternative models that rely on DoD-issued mobile devices. It is cheaper to provision personal devices and reimburse or provide a mobile stipend to employees than to match device turnover at the speed of technological change through government procurement of handsets or tablets. Additionally, ensuring continued modernization through a BYOD model would limit the high costs associated with maintaining outdated infrastructure likely to remain in place if existing procurement policies persist. Furthermore, reductions in overall cost would leave room to provision more devices more frequently under a BYOD model, meaning employees could upgrade their devices as often as they choose without sacrificing DoD connectivity.

Lastly, DoD implementation would provide a proven and secure model for other government agencies with smaller IT budgets. Given the pace of technological change, a number of institutions are seeking to upgrade the mobile devices issued to staff – Android devices and iPhones are the new standard on the Hill, and the White House recently made the switch to iPhones.[18] Setting a strong example of workforce mobility within DoD will show clearly how enterprise-level benefits offered by advanced mobile technology can be maximized in terms of security and cost by a forward-thinking approach. As more government agencies consider how to take advantage of the capabilities that leading-edge mobile devices have to offer, best practices established by DoD can guide cost-effective strategies for adoption.

Where highly regulated DoD models of mobility once mitigated the weaknesses inherent in older generations of mobile devices, now such policies undermine information security as they slow DoD adoption of advanced mobile technology and keep the department from taking advantage of the full host of capabilities mobility has to offer. There is always some level of risk within the field of information technology, and next-generation mobile devices will not be without weaknesses. Yet, given the advances in mobile computing and the capabilities of near future devices, DoD will face greater risks from failing to leverage leading-edge technology than from mobile devices themselves. Implementing a BYOD model of mobility will address this challenge and support the Department of Defense in capitalizing on new mobile capabilities at the speed of change.

A pilot with Marine Light Attack Helicopter Squadron 269 uses a tablet to mark friendly and enemy targets during a 2016 urban close air support exercise in Arizona. (Lance Cpl. Andrew Huff/ U.S. Marine Corps)

Conclusion

In spite of the significant opportunities for technological advancement and benefits to workforce mobility offered by a BYOD model, the Department of Defense is unlikely to abandon the current procurement policy or mobility program to initiate sweeping change. In reality, successfully overcoming bureaucratic impediments and an entrenched culture of risk aversion will require a measured approach.

The initial challenge will be to prove that advanced mobile technology is compatible with DoD security demands in practice. Implementing a small-scale program using a COBO model to issue DoD employees approved COTS handsets and tablets with full access to the features of advanced devices is a viable first step toward the BYOD model. As the technology is verified and the BYOD model gains support, DoD can adjust policy as required and scale up over time, modernizing information technology infrastructure gradually to support and shift more capabilities to mobile devices as appropriate.

In the future, advanced mobile technology will offer different and potentially more significant benefits to consider in operational and battlefield environments. For example, tighter control over data-in-transit will support stronger signature management, enhancing battlefield survivability. DoD experience with adopting next-generation mobile devices in a headquarters environment will be invaluable to determining the best way to integrate and take advantage of new mobile technology in even more sensitive operational settings.

Endnotes

1. "Enterprise Mobility Overview, Solutions, and Benefits – Accenture Digital," Accenture, https://www.accenture.com/us-en/understanding-enterprise-mobility.

2. Tom Bajarin, "The future of pocket computing," Recode, June 16, 2016, http://www.recode.net/2016/6/16/11950372/pocket-computing-wireless-mobile-touchscreen-intelligence; Christina Bonnington, "In Less than Two Years, a Smartphone Could be Your Only Computer," Wired, February 2, 2015, http://www.wired.com/2015/02/smartphone-only-computer/.

3. Sarah Perez, "Google plans to bring password-free logins to Android apps by year end," TechCrunch, May 23, 2016, https://techcrunch.com/2016/05/23/google-plans-to-bring-password-free-logins-to-android-apps-by-year-end/.

4. Thomas Claburn, "Google Taps Machine Learning to Make Smartphones Smarter," InformationWeek, January 29, 2016, http://www.informationweek.com/mobile/mobile-devices/google-taps-machine-learning-to-make-smartphones-smarter/d/d-id/1324090; Ivana Kottasova, "Apple patents technology to block your phone camera," CNN Money, June 30, 2016, http://money.cnn.com/2016/06/30/technology/apple-patent-stop-phone-recording/index.html.

5. Cheryl Pellerin, "DoD CIO Discusses Pentagon Wireless, Mobility Programs," U.S. Department of Defense, July 15, 2015, http://www.defense.gov/News/Article/Article/612649.

6. Andrew Orlowski, "Blackberry chief: We don't have to make phones to make phones," The Register, July 19, 2016, http://www.theregister.co.uk/2016/07/19/blackberry_chen_handset_strategy_nyc/.

7. In a study of enterprise mobility conducted by Accenture in 2015, respondents cited security concerns as the most prevalent obstacle to digital adoption. "Growing the Digital Business: Accenture Mobility Research 2015," Accenture Digital, 2015, https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents14/Accenture-Growing-The-Digital-Business-Acn-Mobility-Research-2015.pdf.

8. Department of Defense Chief Information Officer, DoD CIO Mobility Industry Day Mobility Update/Overview (July 9, 2015), https://www.signup4.net/Upload/CONN15A/DODM12E/DoD_CIO_Mobility_Industry_Day_Overview_FINAL_07092015.pdf; National Information Assurance Partnership, "What is NIAP/CCEVS?," https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm.

9. Kenneth Corbin, "Shadow BYOD runs rampant in federal government," CIO, September 1, 2015, http://www.cio.com/article/2978841/byod/shadow-byod-runs-rampant-in-federal-government.html.

10. Tim Moynihan, "Review: Samsung Galaxy Note 7," Wired, August 16, 2016, http://www.wired.com/2016/08/review-samsung-galaxy-note-7/.

11. "Hardware RoTs are preferred over software RoTs due to their immutability, smaller attack surface, and more reliable behavior." Lily Chen, Joshua Franklin, Andrew Regenscheid, National Institute of Standards and Technology, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft): Recommendations of the National Institute of Standards and Technology, 800-164 (October 2012), 1.

12. "In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport. As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs. The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending. The units look like public data, allowing them to be transmitted across the Internet. Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur." "Techopedia explains Tunneling," Techopedia, https://www.techopedia.com/definition/5402/tunneling.

13. "Enterprise Mobility Overview, Solutions, and Benefits – Accenture Digital."

14. "DoD Mobility Classified Capability – Secret," Defense Information Systems Agency, http://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMCC.

15. Bob Stevens, "Unpacking Terry Halvorsen's 3 reasons for pursuing BYOD," FCW, April 10, 2015, https://fcw.com/articles/2015/04/10/dod-byod.aspx.

16. Digital Services Advisory Group and Federal Chief Information Officers Council, Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs (August 23, 2012), https://www.whitehouse.gov/digitalgov/bring-your-own-device.

17. Department of Defense, Department of Defense Commercial Mobile Device Implementation Plan (February 15, 2013), 16.

18. David Murphy, "U.S. Senate Stops Issuing BlackBerry Devices," PCMag, July 2, 2016, http://www.pcmag.com/news/345803/u-s-senate-stops-issuing-blackberry-devices.

19. Department of Defense Chief Information Officer, DoD CIO Mobility Industry Day Mobility Update/Overview (July 9, 2015),https://www.signup4.net/Upload/CONN15A/DODM12E/DoD_CIO_Mobility_Industry_Day_Overview_FINAL_07092015.pdf; "DoD Mobility Classified Capability – Secret," Defense Information Systems Agency, http://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMCC; "DoD Mobility Program," Defense

Information Systems Agency, http://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility.

20. Lily Chen, Joshua Franklin, Andrew Regenscheid, National Institute of Standards and Technology, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft): Recommendations of the National Institute of Standards and Technology, 800-164 (October 2012), 11.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org**

Bold. Innovative. Bipartisan.