On July 13, 2015, Deputies asked the encryption working group to prepare for Principals' consideration guidance on (1) key trade-offs identified through its analysis of possible technical approaches; and (2) the lessons learned from that analysis. This document provides that assessment and further identifies technical challenges for which the working group was unable to identify solutions and potential policy principles that could guide any engagement by the United States Government with industry on encryption issues. To facilitate Principals' analysis and discussion, this document includes the four technical approaches to implementing accessible encryption developed by the working group developed. However, these approaches are intended as proofs-of-concept and Deputies agree that the approaches should not be advanced as affirmative Administration proposals or shared outside the United States Government.

Lessons Learned. Encryption working group participants have identified four key lessons that should inform any consideration of technical proposals to enable targeted lawful access to encrypted data.

There is no "one-size-fits-all" technical approach. No single approach can enable access to encrypted information across all media and providers. Each type of encryption will require unique technical approaches, and each particular company would need to implement approaches specifc to their implementation of encryption in the products and services it offers. Further, enabling lawful access to some forms of encrypted data, should companies be willing to do so, will be easier with some implementations than others.

Different encryption implementations require different approaches. From a technical perspective, encryption can be divided into three categories: the encryption of data stored on devices held by consumers; the encryption of communications in transit between parties; and the encryption of data stored in remote locations (e.g., cloud-based storage of backups). Each type of encryption carries different security risks, policy implications, and technical challenges - and maintaining clarity in technical and policy discussions is essential to identifying potential options. For example, one approach to enabling access to data on devices could be through limiting to only those with physical access to the device, which reduces the security risks of such access and limits the ability for abuse. Similarly, the nature of communications encryption poses particular challenges to law enforcement access solutions that do not exist for stored data (whether in the cloud or on devices). .

Intended use cases should drive proposed technical approaches. Law enforcement may seek access to encrypted data in a variety of scenarios, and the particular circumstances will substantially change the requirements of how a provider might enable that access. For example, law enforcement seeking to use encrypted data to stop an impending attack or crime needs rapid access whilelaw enforcement seeking to use data on a seized device to make a case against a defendant could accept a slower solution. Similarly, efforts to compel access to encrypted data held by sophisticated criminals like terrorists and organized crime may be unsuccessful if the fact that such compulsion is possible is widely known because such criminals will choose to use inaccessible alternatives. On the other hand, unsophisticated criminals or individuals responsible for crimes of passion, may be less likely to switch to technology products and services that are inaccessible to law enforcement.

Technical approaches can be enforced in multiple ways. The technical requirements of a particular proposed solution (for instance, that law enforcement may only access data on a single device as part of each request) could be enforced in multiple ways. It could be enforced through a law, through Executive branch policy, or through technological limitations built into the device or service itself. However, some technologists, civil society, and companies may perceive any government access as an attempt to obtain widespread, non-targeted access for bulk collection purposes. Accordingly, those communities almost certainly will be unlikely to trust limitations enforced through policy or law, and will be more likely to be satisfied by those enforced through technology.

Technical Challenges. The working group also identified several technical challenges for which there is no clear solution. Although technical approaches to enable lawful access to encrypted data may be able to mitigate some of the public safety challenges posed by encryption, these challenges mean that inaccessible encryption will always be available to malicious actors.

Strong encryption is increasingly available in global technology products and services. Unlike the "crypto wars" of the 1990s, encryption is no longer solely available to governments. Established companies and independent developers in many countries around the world are developing encrypted products and services. Further, encryption can be implemented purely through software and effective encryption implementations are increasingly available in the public domain. As a result, encrypted products and services will always be available to malicious actors, including in countries that do not adopt an accessibility regime.

Encrypted products and services often use open source software for implementation. Many encryption solutions are open-source projects developed by communities of volunteers that are based in multiple countries. For example, the predominant implementation of the encryption protocol used to secure web sites for e-commerce transactions is open source. Most of these solutions are made available free of cost, and are not distributed by any single institution, but shared on a peer-to-peer basis. As a result, there may be no central authority that can update these solutions to comply with any requirements for implementing encryption in a manner that would support law enforcement access.

Inaccessible encryption can be layered on top of accessible encryption. Because encryption solutions are often implemented through software, individuals using a device with accessible encryption can easily install an inaccessible software encryption solution on the device. For example, if Apple or Google were to change their mobile phones to allow for decryption of the device pursuant to lawful process, a user could still download a mobile application that could allow for encrypted communications (e.g., Skype). Layered encryption means that, even if all core U.S. services and devices have accessible encryption, individuals will be able to defeat attempts to access their information.

Proposed Policy Principles

Deputies agreed that attempts to build cooperation with industry, vice proposing specific technical solutions, will offer the most successful option for making progress on this issue. In particular, given industry and civil society's combative reaction to government statements to date, any proposed solution almost certainly would quickly become a focal point for attacks and the basis of further entrenchment by opposed parties. Rather than sparking more discussion, government-proposed technical approaches would almost certainly be perceived as proposals to introduce "backdoors" or vulnerabilities in technology products and services and increase tensions rather build cooperation.

However, if the United States Government were to provide a set of principles it intends to adhere to in developing its encryption policy, such a document could spark public debate. Proposing such principles would not be without risk, as some constituencies may not distinguish between principles and specific technical approaches. As a result, these principles could come under attack, but could also serve to focus public or private conversation on practicalities and policy trade-offs rather than whether the government is seeking to weaken encryption or introduce vulnerabilities into technology products and services.

Based on the lessons learned from the initial technical review, the encryption working group has developed a set of principles that could guide the United States Government's engagement with the private sector on encryption. While all of the principles should inform private discussions with industry, some, all, or none of them could be incorporated into anypublic debate.

1. *No bulk collection*. Any approach to enable lawful access should focus on enabling targeted - as opposed to bulk – access to decrypted information.

2. *No unilateral government access*. Approaches should not provide "golden keys" to government or allow government to access decrypted information without the assistance of a third party.

3. *Technologically-enforced limits*. To the extent possible, approaches should rely on technology, rather than procedural protections, to enforce constraints on government access.

4. *International adoption*. The United States Government will accept that any U.S.-proposed solution will be adopted by other countries.

5. *Maximize security and minimize complexity*. Any accessibility regime carries the inherent risk that a malicious actor could exploit that accessibility for malicious ends. As a result, any accessibility regime should be designed to minimize complexity (a key factor that increases risk of vulnerability) and maximize security.

6. *Minimize impact of malicious exploitation.* No technical approach can be implemented in a manner that guarantees perfect security. Accordingly, any accessibility regime must be designed to limit the impact of a successful exploit by a malicious actor. For instance, a device access regime that requires physical access to the device would limit the impact of an exploit because a malicious actor would have to have physical possession of a targeted device.

7. *Minimize negative impact on innovation.* Certain access regimes could limit technical innovation by closing the door to certain types of encryption solutions. For example, current best practices for communications encryption requires that each new message be encrypted using a distinct key - a principle called forward secrecy that mitigates the consequences of an exploit by ensuring that any single key only exposes a single communication. A technical approach that implemented accessible encryption in a manner that makes forward secrecy impossible would limit innovation and hamper efforts to better secure communications. In this vein, any accessibility requirement should be designed in such a way that it minimizes any negative impact on innovation.

8. *No "one size fits all" approach.* No single accessible solution that could work for all types of encryption or all developers. Providers, not the government should be responsible for determining how to design any feasible approaches into their products and services.

Avoid undermining trust in security. The modern Internet ecosystem relies on all participants trusting the security of their communications and data. Any technical approach should be tailored to avoid undermining this trust.

9.

Technical "Proofs of Concept"

Technical experts in the working group developed several proof-of-concept technical approaches that could theoretically enable access to some types of encrypted data. Working group participants agreed that all of these proposals were technically feasible, although they disagreed as to the value and viability of each of the solutions. Further, working group participants agreed that these proposals should be seen as only examples, and would need to go through substantial revision and refinement if they were to be further pursued.

Provider-enabled access to encrypted devices based on physical control of the device. For this approach, providers would modify the hardware of their devices to include an independent, physical, encrypted port. The provider would maintain a separate set of keys for its customers' devices that would enable it to decrypt those devices, but only if it had physical access to the device itself. If law enforcement seized an encrypted device that it could not access, it would secure lawful process from a U.S. court and submit the device itself, along with the lawful process, to the provider. The provider would use its secondary key to unlock the device, and provide the resulting data back to law enforcement. Making a hardware modification would impose significant cost on U.S. manufacturers, but requiring physical access to enable decryption substantially reduces the cybersecurity risk of a secondary access point, and limits the risk of abuse by malicious actors and foreign government entities. This solution would provide access only to devices (although some communications stored on the device could be accessible as well), and would not prevent a customer from installing a secondary layer of encryption on top of the device encryption.

Provider-enabled remote access to encrypted devices through current update procedures. Virtually all consumer devices include the capability to remotely download and install updates to their operating system and applications. For this approach, law enforcement would use lawful process to compel providers to use their remote update capability to insert law enforcement software into a targeted device. Once inserted, such software could enable far-reaching access to and control of the targeted device. This proposal would not require physical modification of devices, and so would likely be less costly for providers to implement. It would also enable remote access, and make surreptitious access much less costly. However, its use could call into question the trustworthiness of established software update channels. Individual users, concerned about remote access to their devices, could choose to turn off software updates, rendering their devices significantly less secure as time passed and vulnerabilities were discovered by not patched.

Remote access enabled only when multiple parties, each of which holds a partial key, participate. In this approach, a secondary decryption key is divided across multiple recovery parties.

These parties would provide their sub-keys either to the provider or to law enforcement under court order to enable reconstruction of the encryption key and decryption of the data. This approach would enable remote and surreptitious access to data stored both in devices and remote databases. It would also limit the risk of exploit by requiring any attacker to infiltrate multiple recovery entities to secure a complete recovery key. However, it is important to note that this approach would be complex to implement and maintain, as it would require a network of independent recovery parties which could then be validated by trusted third parties.

Remote access to data stored on encrypted devices enabled by providers implementing a "forced backup" of the data to an alternate, accessible location. The approach relies on providers being able to remotely backup information stored in an encrypted location to a different location that is not encrypted. Pursuant to lawful process, the provider would turn on remote backup, and provide the resulting backed-up information to law enforcement. This solution could be implemented with notice to the customer (for instance, a dialog box on their device could indicate that remote backup is being enabled, and could indicate that it is happening in response to a law enforcement request or not), or could be done surreptitiously. For many providers, enabling this proposal would require designing a new backup channel, or substantially modifying an existing channel.