LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies

Transmittal Letter

Dear Mr. President:

We are honored to present you with the Final Report of the Review Group on Intelligence and Communications Technologies. Consistent with your memorandum of August 27, 2013, our recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.

We have emphasized the need to develop principles designed to create strong foundations for the future. Although we have explored past and current practices, and while that exploration has informed our recommendations, this Report should not be taken as a general review of, or as an attempt to provide a detailed assessment of, those practices. Nor have we generally engaged budgetary questions (although some of our recommendations would have budgetary implications).

We recognize that our forty-six recommendations, developed over a relatively short period of time, will require careful assessment by a wide range of relevant officials, with close reference to the likely consequences. Our goal has been to establish broad understandings and principles that

can provide helpful orientation during the coming months, years, and decades.

We are hopeful that this Final Report might prove helpful to you, to Congress, to the American people, and to leaders and citizens of diverse nations during continuing explorations of these important questions.

Richard A. Clarke

Michael J. Morell

Geoffrey R. Stone

Cass R. Sunstein

Peter Swire

Recommendations

Recommendation 1

We recommend that section 215 should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if:

(1) it finds that the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and

(2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 2

We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

(1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and

(2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 3

We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.

Recommendation 4

We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

Recommendation 5

We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intellience Surveillance Court that meets the requirements set forth in Recommendation 1.

Recommendation 6

We recommend that the government should commission a study of the legal and policy options for assessing the distinction between meta-data and other types of information. The study should include

technological experts and persons with a diverse range of perspectives, including experts about the missions of intelligence and law enforcement agencies and about privacy and civil liberties.

Recommendation 7

We recommend that legislation should be enacted requiring that detailed information about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

Recommendation 8

We recommend that:

(1) legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten

the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;

(2) nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and

(3) nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality.

Recommendation 9

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 10

We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National

Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 11

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be *substantially* impaired if our enemies were to know of its existence.

Recommendation 12

We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person:

(1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;

(2) any information about the United States person may not be used in evidence in any proceeding against that United States person;

(3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

Recommendation 13

We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance:

(1) must be authorized by duly enacted laws or properly authorized executive orders;

(2) must be directed *exclusively* at the national security of the United States or our allies;

(3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries; and

(4) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies.

In addition, the US Government should make clear that such surveillance:

(1) must not target any non-United States person located outside of the United States based solely on that person's political views or religious convictions; and

(2) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

Recommendation 14

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

Recommendation 15

We recommend that the National Security Agency should have a limited statutory emergency authority to continue to track known targets of counterterrorism surveillance when they first enter the United States,

until the Foreign Intelligence Surveillance Court has time to issue an order authorizing continuing surveillance inside the United States.

Recommendation 16

We recommend that the President should create a new process requiring high-level approval of all sensitive intelligence requirements and the methods the Intelligence Community will use to meet them. This process should, among other things, identify both the uses and limits of surveillance on foreign leaders and in foreign nations. A small staff of policy and intelligence professionals should review intelligence collection for sensitive activities on an ongoing basis throughout the year and advise the National Security Council Deputies and Principals when they believe that an unscheduled review by them may be warranted.

Recommendation 17

We recommend that:

(1) senior policymakers should review not only the requirements in Tier One and Tier Two of the National Intelligence Priorities Framework, but also any other requirements that they define as sensitive;

(2) senior policymakers should review the methods and targets of collection on requirements in any Tier that they deem sensitive; and

(3) senior policymakers from the federal agencies with responsibility for US economic interests should participate in

the review process because disclosures of classified information can have detrimental effects on US economic interests.

Recommendation 18

We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees.

Recommendation 19

We recommend that decisions to engage in surveillance of foreign leaders should consider the following criteria:

(1) Is there a need to engage in such surveillance in order to assess significant threats to our national security?

(2) Is the other nation one with whom we share values and interests, with whom we have a cooperative relationship, and whose leaders we should accord a high degree of respect and deference?

(3) Is there a reason to believe that the foreign leader may be being duplicitous in dealing with senior US officials or is attempting to hide information relevant to national security concerns from the US?

(4) Are there other collection means or collection targets that could reliably reveal the needed information?

(5) What would be the negative effects if the leader became aware of the US collection, or if citizens of the relevant nation became so aware?

Recommendation 20

We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection.

Recommendation 21

We recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections). The criteria should include:

(1) shared national security objectives;

(2) a close, open, honest, and cooperative relationship between senior-level policy officials; and

(3) a relationship between intelligence services characterized both by the sharing of intelligence information and analytic thinking and by operational cooperation against critical targets of joint national security concern. Discussions of such understandings or arrangements should be done between relevant intelligence communities, with senior policy-level oversight.

Recommendation 22

We recommend that:

(1) the Director of the National Security Agency should be a Senate-confirmed position;

(2) civilians should be eligible to hold that position; and

(3) the President should give serious consideration to making the next Director of the National Security Agency a civilian.

Recommendation 23

We recommend that the National Security Agency should be clearly designated as a foreign intelligence organization; missions other than foreign intelligence collection should generally be reassigned elsewhere.

Recommendation 24

We recommend that the head of the military unit, US Cyber Command, and the Director of the National Security Agency should not be a single official.

Recommendation 25

We recommend that the Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

Recommendation 26

We recommend the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget.

Recommendation 27

We recommend that:

(1) The charter of the Privacy and Civil Liberties Oversight Board should be modified to create a new and strengthened agency, the Civil Liberties and Privacy Protection Board, that can oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes;

(2) The Civil Liberties and Privacy Protection Board should be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community;

(3) An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies; and

(4) Some compliance functions, similar to outside auditor functions in corporations, should be shifted from the National Security Agency and perhaps other intelligence agencies to the Civil Liberties and Privacy Protection Board.

Recommendation 28

We recommend that:

(1) Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;

(2) the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;

(3) the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and

(4) Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices.

Recommendation 29

We recommend that, regarding encryption, the US Government should:

(1) fully support and not undermine efforts to create encryption standards;

(2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and

(3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

(1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry;

(2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;

(3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers;

(4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows.

Recommendation 32

We recommend that there be an Assistant Secretary of State to lead diplomacy of international information technology issues.

Recommendation 33

We recommend that as part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

Recommendation 34

We recommend that the US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

Recommendation 35

We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are

statistically reliable, cost-effective, and protective of privacy and civil liberties.

Recommendation 36

We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Recommendation 37

We recommend that the US Government should move toward a system in which background investigations relating to the vetting of personnel for security clearance are performed solely by US Government employees or by a non-profit, private sector corporation.

Recommendation 38

We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things as changes in credit ratings or any arrests or court proceedings.

Recommendation 39

We recommend that security clearances should be more highly differentiated, including the creation of "administrative access" clearances that allow for support and information technology personnel

to have the access they need without granting them unnecessary access to substantive policy or intelligence material.

Recommendation 40

We recommend that the US Government should institute a demonstration project in which personnel with security clearances would be given an Access Score, based upon the sensitivity of the information to which they have access and the number and sensitivity of Special Access Programs and Compartmented Material clearances they have. Such an Access Score should be periodically updated.

Recommendation 41

We recommend that the "need-to-share" or "need-to-know" models should be replaced with a Work-Related Access model, which would ensure that all personnel whose role requires access to specific information have such access, without making the data more generally available to cleared personnel who are merely interested.

Recommendation 42

We recommend that the Government networks carrying Secret and higher classification information should use the best available cyber security hardware, software, and procedural protections against both external and internal threats. The National Security Advisor and the Director of the Office of Management and Budget should annually report to the President on the implementation of this standard. All networks carrying classified data, including those in contractor corporations, should be subject to a Network Continuous Monitoring

Program, similar to the EINSTEIN 3 and TUTELAGE programs, to record network traffic for real time and subsequent review to detect anomalous activity, malicious actions, and data breaches.

Recommendation 43

We recommend that the President's prior directions to improve the security of classified networks, Executive Order 13587, should be fully implemented as soon as possible.

Recommendation 44

We recommend that the National Security Council Principals Committee should annually meet to review the state of security of US Government networks carrying classified information, programs to improve such security, and evolving threats to such networks. An interagency "Red Team" should report annually to the Principals with an independent, "second opinion" on the state of security of the classified information networks.

Recommendation 45

We recommend that all US agencies and departments with classified information should expand their use of software, hardware, and procedures that limit access to documents and data to those specifically authorized to have access to them. The US Government should fund the development of, procure, and widely use on classified networks improved Information Rights Management software to control the dissemination of classified data in a way that provides greater restrictions on access and use, as well as an audit trail of such use.

Recommendation 46

We recommend the use of cost-benefit analysis and risk-management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures.