– Coming In from the Surveillance Cold –

–

Former NSA Insiders
Make Recommendations to Roll Back Government Surveillance

Recommendations to Accompany Our Open Memorandum to the President

Open Memorandum: http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong/

Executive Summary

Legislation, judicial review through the FISA Court, and testimony have failed utterly in terms of providing meaningful oversight - both historically and currently – over NSA operations. For this reason, we put forth the following set of recommendations.

Recommendations:

1 Foreign Intelligence Surveillance Court (FISC): Reject ability to interpret Constitution, requiring that FISC rely on US District, Appeals and Supreme Court precedents; make all rulings public, with the legitimacy of any security redactions verified independently; revoke 2008 FISA Amendments Act and other restrictions on FISC so that it may again reject applications for warrants on substantive grounds; provide for expert attorneys arguing the case for US residents' privacy and for application of the national security qualification regarding foreign collection.

2 Revoke the AUMF (Authorization for Use of Military Force) invoked to justify use of extraordinary alleged Presidential war powers.

3 Restore the Foreign Intelligence Surveillance Act of 1978 to its original state augmented with a provision permitting the collection and storage of foreign-to-domestic and domestic-to-foreign communications granted under E.O. 12333 Part II, Section 2.C. as authorized by both the Attorney General and Judiciary Committees of both the House and Senate and halt bulk collection/storage of domestic communications conducted under all other authorities. Caveat: These permissions are appropriate only if congress and the judicial branch are able to verify compliance with them through the use of audit trails accounting for each access to sensitive databases supporting NSA operations, and the cradle-to-grave disposition of data used for any purpose other than maintenance.

4 Immediately outlaw the business records, un-notified searches and general warrants practices under PATRIOT Act, FISA, FISC and any other precedents, requiring individual court warrants based on probable cause to acquire the records of US residents. Mandate that individual companies turning over records to the federal government publish annual statistics on the number and types of records and they notify their affected customers as a norm within [90] days and in exceptional circumstances within [180] days. Eliminate other clauses with obvious abuses immediately and after a thorough independent investigation of post-9/11 practices, eliminate or revise, reduce and clarify all other associated legislation by June 2015. Caveat: These permissions are appropriate only if congress and the judicial branch are able to verify compliance with them through the use of audit trails accounting for each access to sensitive databases supporting NSA operations, and the cradle-to-grave disposition of data used for any purpose other than maintenance.

5 Update privacy rights along lines of European standards, including, e.g.: establishing the privacy of records required of customers in order to conduct modern life and business; modifying HIPAA to require an individual warrant based on probable cause for "national security" access to medical records; reinforcing the privacy of IRS and other selected federal, state and local government records; etc.

6 Create severe penalties for individual government officials who violate the privacy rights of US residents, including loss of security clearance, fines, jail sentences and complete loss of pension rights or partial loss for accruals during the years of participation, dependent upon the leadership position of the person in question and their demonstrable effort to counter unconstitutional or illegal practices. Enforce the punishments and penalties under existing FISA law.

7 Apply effective whistleblower protections to employees, contractors and subcontractors of national security agencies and establish generous rewards for information with access to the courts for cause of action.

8 Further bans on bulk collection against foreign private individuals and entities that are not closely associated with national security threat to the US or validated Information Needs. Caveat: These permissions are appropriate only if congress and the judicial branch are able to verify compliance with them through the use of audit trails accounting for each access to sensitive databases supporting NSA operations, and the cradle-to-grave disposition of data used for any purpose other than maintenance.

9 Outlaw national security letters and for US citizens require a Federal District Court warrant based on individual probable cause standard.

10 Outlaw use of foreign partner agencies to circumvent US laws and ban US agencies from aiding foreign partner agencies in circumventing their own laws, and apply individual penalties to such activities.

11 Zero-base the NSA, CIA and FBI budgets and cut them substantially by eliminating unconstitutional or illegal programs. Require software that selects individual communications of national security interest, eliminate bulk collection of metadata or content, and render unlawful dependence on communications companies for normal collection and decryption access, seeking their cooperation only in extraordinary, limited circumstances with the approval of both the House and Senate Judiciary Committees.

12 Encrypt incidentally collected domestic communications and metadata until an individual warrant based on probable cause is obtained.

13 Install automated tracking technology of accesses to and manipulation of NSA (and related FBI and CIA) databases.

14 Establish a Special Independent Signals Investigatory Body including but not limited to Members of Congress, Tech industry experts, Privacy experts, et al with subpoena powers, that investigates the historical evolution of all post-9/11 intelligence practices of questionable legality across the board and reports comprehensively to the public within a year. Intelligence agencies may recommend classification and redactions for the report, but final decisions are to be made by the Board itself with the need for democratic transparency trumping an equal argument for withholding.

15 An independent and permanent Signals Technical Team (STT) with continuous and unquestioned access to: all NSA (and related FBI/CIA) databases and tracking of accesses to them, adherence to laws, partnerships, contracts, development activity, operations, dissemination, minimization, etc. This Team is established to inform FISC, relevant Congressional committees (i.e., Judicial, Oversight, and Intelligence) and the Special Independent Investigatory Body with independent confirmation of legal and constitutional activities, efficiency of expenditures, and operations. Its membership shall be composed of technical experts not previously employed by NSA/FBI/CIA. The STT shall also be available to whistleblowers and other experts with full confidentiality, along with Congressional committees and the FISC itself.

16 Investigate and reveal publicly what non-communications data is collected on Americans under national security aegis by NSA and other federal agencies, under what circumstances and stipulating rules of storage, access and use.

17 Reveal agencies with access to, copies of or information obtained from these NSA databases, their rules for storage, database searches and information use, and officials and methodology responsible for enforcing and verifying adherence to the rules. Establish whether the databases are being used for non-foreign intelligence purposes, whether cover stories have been used to construct a fake evidence trail, and whether and when ethical norms and discovery rules have been violated during any and all court proceedings.

18 Establish and publicize historical and current remuneration to individual communications and other companies and agencies, by year, for access to and/or copies of their data.

19 Reveal all "upstream" collection, storage and distribution capabilities.

20 Much of the public discourse emanating from the executive branch related to the Edward Snowden revelations has been surrounded with obfuscation intended to mislead the public. To minimize miscommunication in congressional hearings, all communications-related terminology referencing any aspect of intelligence collection, processing, storage, analysis, reporting, and dissemination shall be defined and codified in accordance with DoDAF AV-2 Integrated Dictionary standards and approved and baselined by the House and Senate Judiciary Committees. All subsequent hearings with intelligence officials addressing such activities shall employ language defined in that AV-2.

21 Only collect content that is associated with known “bad guys” and those within the zone of suspicion (those within 2 degrees of separation from a known “bad guy”).

Signatories

William Binney, former Technical Director, World Geopolitical & Military Analysis; Co-founder of the SIGINT Automation Research Center.

Thomas Drake, former Defense Intelligence Senior Executive Service, NSA

Edward Loomis, former Chief, SIGINT Automation Research Center, NSA

J. Kirk Wiebe, former Senior Analyst, SIGINT Automation Research Center, NSA

PREPARED UNDER AUSPICES OF AD HOC STEERING GROUP
VETERAN INTELLIGENCE PROFESSIONALS FOR SANITY

Ray McGovern, CIA analyst/Presidential Briefer, (ret.)

Elizabeth Murray, Deputy National Intelligence Officer for Near East (ret.)

Coleen Rowley, Minneapolis Legal Counsel & Special Agent, FBI (ret.)

Daniel Ellsberg, Former State Dept. & Defense Dept. Official (VIPS Associate)