CENTER FOR SECURITY POLICY | OCCASIONAL PAPER SERIES

A Critique of the Recommendations by the President's Review Group on Intelligence and Communication Technologies

A Center for Security Policy Analysis

Fred Fleitz and Clare Lopez

1/13/2014

Fred Fleitz served in U.S. national security positions for 25 years at the CIA, DIA, Department of State and the House Intelligence Committee staff. Clare Lopez is a strategic policy and intelligence expert with a focus on national defense, Islam, Iran, and counterterrorism. Both serve as senior fellows at the Center for Security Policy. This paper is a critique of the Presidents Review Group on Intelligence and Communications Technologies report, which recommended reforms on intelligence, technology, and privacy issues, and provides alternative recommendations.

Last August President Barack Obama named a panel, the Review Group on Intelligence and Communication Technologies, in response to the national debate that followed the illegal disclosure of classified documents by former NSA technician Edward Snowden, and Snowden's misrepresentations about NSA intelligence practices. The Review Group issued a report with recommended reforms on intelligence, technology, and privacy issues on December 12. On January 17th, President Obama will announce what reforms he will implement in response to the Review Group report.

The Center for Security Policy (CSP) disagrees with most of the Review Group's recommendations and believes many would undermine U.S national security. To help inform this debate and the President's decision, we have drafted this critique of the Review Group's recommendations and provided alternative recommendations.

This memo will be followed later this week by a joint statement of principles by national security professionals to help guide President Obama's response to the Review Group report.

1) Review Group Recommendations on NSA Metadata Program Would Eviscerate an Important Counterterrorism Program and Create Real Privacy Concerns

CSP's Recommendation

We agree with the Review Group that steps need to be taken to reassure the American people about the legality of the Patriot Act Section 215 and related programs and that they are not a threat to privacy. However, the Group's recommendations would seriously weaken the program's effectiveness and would create real privacy concerns by having private parties – in addition to telephone companies – hold telephone metadata of Americans instead of NSA.

We believe the best way to address concerns about the 215 program is through bipartisan legislation under discussion in the congressional intelligence committees. The Senate Select Intelligence Committee (SSCI) attempted to do this when it passed the FISA Improvements Act of 2013 by a decisive vote of 11 to 4 last October. The House Intelligence Committee reportedly is working on a similar bill. The SSCI bill would codify a requirement for NSA analysts to have a "reasonable articulable suspicion" that a phone number is associated with terrorism to query the metadata database. The bill would also impose a five-year limit on the retention of bulk communication records acquired under Section 215 of the Patriot Act and require Attorney General approval to query records that are older than three years. It calls for closer review by the FISA court and additional annual reports to the committee on 215 queries.

We believe the FISA Improvements Act is a step in the right direction and should become the basis of a House-Senate bill addressed to the 215 program. We ask the President to work with the congressional intelligence committees on new legislation to bolster the 215 program and not adopt the Review Panel's recommendations.

The Review Group's Recommendations

The first 11 recommendations and Recommendation 20 in the Review Group report address the principal reason for its report: NSA collection of telephone metadata records as authorized under Section 215 of the Patriot Act which allows NSA to hold and search these phone records to find intelligence on terrorist-related connections. Leaks about the 215 program by Edward Snowden have caused a firestorm of criticism that it violates the privacy rights of Americans and allows NSA to monitor their personal phone calls. In fact, this program does not allow the government to monitor phone calls, only phone records which several judges have concluded are not subject to privacy protections. **While the Review Group would keep the 215 program in place, we oppose all of its recommendations on this program as they would place so many limitations on the metadata program that it would be rendered virtually useless. We also believe these recommendations address privacy concerns that lack validity and would actually increase the potential for real privacy violations.**

U.S. District Judge for the District of Columbia Richard Leon was highly critical of the 215 program in his December 16 decision *Klayman vs Obama,* writing that it is probably a violation of the Fourth Amendment. In a December 27 decision, *ACLU vs Clapper*, Southern District of New York Judge William H. Pauley came to the opposite conclusion, ruling that the 215 effort is a lawful and vital counterterrorism intelligence program which he described as the government's "counterpunch connecting fragmented and fleeting communications to re-construct and eliminate al-Qaeda's terror network."

The constitutionality of the 215 program is based on the 1979 Supreme Court case *Smith vs. Maryland* and has been upheld through 36 challenges before 16 different judges. The review panel questions whether the Smith decision is still good law. We believe it is and that the Supreme Court is likely to uphold 215 based on this decision when it ultimately rules on appeals of the *Klayman* and *ACLU* decisions.

Allegations have been made that this program is overly broad, gives NSA too much discretion as to how and when to employ it, and has been subject to insufficient oversight by the Foreign Surveillance Intelligence Court (FISC) and the congressional intelligence committees. However, the Review Group, Judge Leon and Judge Pauley all agree that there is no evidence that the 215 program has been abused.

Although the Review Group report states that the 215 program "was not essential to preventing terrorist attacks," Review Group member Michael Morell contradicted this finding just after the report was issued when he said in a December 27, 2013 Washington post op-ed that if the metadata program had been in place before September 2001, "it would likely have prevented 9/11" and "has the potential to prevent the next 9/11."

Another significant endorsement of the 215 program came from a bipartisan statement on December 20, 2013 by the top four members of the House and Senate intelligence committees in which they strongly disagreed with the panel's recommendations. This letter said:

> "The NSA's metadata program is a valuable analytical tool that assists intelligence personnel in their efforts to efficiently 'connect the dots' on emerging or current terrorist threats directed against Americans in the United States. The necessity of this program cannot be measured merely by the number of terrorist attacks disrupted, but must also take into account the extent to which it contributes to the overall efforts of intelligence professionals to quickly respond to, and prevent, rapidly emerging terrorist threats."

We believe this bipartisan statement by members of Congress who understand the metadata program and have closely overseen it for several years should guide President Obama's decision on any steps he chooses to reform it.

The recommendations of the Review Group are not based on abuses or malfeasance. They are based on theoretical abuses of this program, such as gathering metadata to cull personal information like medical records. This is no indication that such an abuse has ever been contemplated, much less carried out. Moreover, the 22 people who have access to the metadata database are closely monitored and forbidden to use it in any fashion other than against suspect telephone numbers.

The most troubling rationale offered by the Review Group for these and other recommendations is to recommend dramatic changes because the potential for abuse "can significantly undermine public trust." That reasoning can be applied to any intelligence program, and indeed to any law enforcement activity: the police officer could beat an innocent citizen with his nightstick, or shoot such a citizen with his pistol; that is not an argument in favor of confiscating police nightsticks or pistols. Indeed, the Review Group concedes, even as it fails to appreciate, that "the degree of oversight and control by high-level officials, legislative members and the judiciary" makes U.S. intelligence collection "unique."

The Review Group makes 12 recommendations which we believe would weaken the 215 program.

Recommendations 1 to 4 would place severe limitations on the issuance of 215 orders and National Security letters. **We oppose these recommendations because we regard them as unwarranted steps that would create new legal obstacles to quickly obtaining Section 215 orders to address urgent national security threats, especially potential terrorist attacks.**

Recommendations 4 and 5 would bar the government from collecting and holding metadata and call for a new system under which metadata would instead be held either by private providers or by a private third party. **We oppose these recommendations because they would create major obstacles to NSA obtaining quick access to the full range of data needed for this program to be effective. We also believe that allowing private parties to hold this data raises the real possibility of increased privacy and national security risks since this information would be kept on less secure servers in numerous locations. A much larger set of people would need to manage this data and would not be subject to NSA's clearance procedures. This would increase new security and privacy vulnerabilities.**

Recommendations 6 to 11 question the legal basis of the 215 program and call for additional oversight and public disclosures. **We oppose these recommendations because we believe the legal justification of this program is not in question and because it is already subject to robust oversight by the congressional intelligence committees and the FISA court. We believe the public disclosures called for in these recommendations would do little to answer critics of these programs but would provide damaging insights on how it is being conducted to America's adversaries, especially terrorist groups.**

Recommendation 20 proposes that the U.S. government develop a software alternative to the 215 program. **We reject this recommendation as unrealistic and laden with potential for abuse if software is sought to be substituted for sound human judgment.**

2) Expanding U.S. Privacy Rights to Non-U.S. Persons Outside the United States is a Dangerous Proposal

CSP's Recommendation

We categorically reject the notions of according U.S. privacy rights to non-U.S. persons outside the United States and barring intelligence agencies from collection against foreign persons based on their religious or political beliefs. These are the worst recommendations by the Review Group and take no account of the nature of foreign intelligence. They also find no support in the U.S. Constitution.

While we oppose the Review Group's proposals to restrict foreign intelligence collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA) as an overreaction to European criticism in the aftermath of Snowden's leaks, we agree that administrative steps should be taken to ensure that politically sensitive intelligence collection, such as eavesdropping on the cellphones of European leaders, is subject to closer senior level review by NSA officials.

We endorse language in the Senate Intelligence Committee's FISA Improvements Act of 2013 that would mandate that NSA analysts seeking collection under 702 involving a U.S. person's name or email must have an articulable foreign intelligence purpose and that a record explaining that purpose will be provided to the FISA Court and Congress. We believe this language is sufficient to address concerns about 702 and we applaud the Senate Intelligence Committee for resisting calls to hamstring 702 collection with provisions to limit collection against non-U.S. targets outside of the United States.

Both the Senate Intelligence Committee and the Review Group have proposed a temporary extension of 702 authority to track intelligence targets when they enter the United States. This is a gap in the law and should be addressed; indeed, this gap accounts for most of the purported violations of guidelines by NSA when non-U.S. persons properly under surveillance enter the United States. Both recommendations call for this authority to be extended to give U.S. officials time to obtain a FISA Court order to continue 702 surveillance inside the Unites States. We

favor the Senate language because it does not limit foreign targets to terrorist suspects and would give the government seven days to obtain a new FISA order as opposed to only 72 hours by the Review Group.

Concerning Recommendation 21, we are sympathetic to calls by German and French officials to add their countries to the "five eyes" intelligence cooperation agreement that currently exists between the United States, the United Kingdom, Canada, Australia and New Zealand. Under this agreement, these states share a significant amount of intelligence and have agreed not to spy on each another. We believe due to increased cooperation on international threats such as counterterrorism and the Iranian nuclear program that Germany and France may one day join the five-eyes group. Before U.S. officials agree to this, however, they must first consider how EU integration would affect increasing intelligence sharing with Germany and France and significant policy differences between these two states and Washington in the recent past. This includes German and French officials aligning with Moscow against the United States during the Iraq War.

The Review Group's Recommendations

Recommendations 12-14 are in response to the global uproar over NSA electronic surveillance of non-U.S. persons under Section 702 of FISA due to the Snowden leaks. Reports that NSA has intercepted huge amounts of electronic communications of Europeans as well as the cell phone of German Chancellor Angela Merkel have driven this debate. In response, the Review Group contends that "significant steps should be taken to protect the privacy of non-US persons" and calls for codes of conduct between foreign intelligence agencies on electronic surveillance against foreign citizens. **We oppose these recommendations because they ignore the realities of intelligence in the modern world and believe they would provide an enormous benefit to U.S. adversaries and foreign intelligence services by tying the hands of U.S. intelligence agencies.**

We live in a dangerous world and we need aggressive intelligence collection efforts to protect our security and freedom. The idea of extending privacy rights under U.S. law and the U.S. Constitution to foreign persons and signing international "no-spy" agreements to limit surveillance of foreign citizens reflects a naïve and dangerous world view. America's adversaries will never agree to such arrangements. Moreover, even striking such agreements with friendly European governments is problematic as many of them have weak records with respect to pursuing terrorist suspects and have allowed too many such suspects to settle in their countries.

Recommendations 12 and 13 would put significant limitations on electronic surveillance of non-U.S. persons outside the United States. **We oppose these recommendations because they would ban abuses that have not occurred and would put unnecessary restrictions on US intelligence collection that already is well-regulated and subject to close oversight. Additional restrictions like these would limit the flexibility and speed with which NSA could address urgent national security threats. Banning U.S. intelligence agencies from considering political or religious convictions would make it difficult to obtain intelligence on Islamist extremists like al Qaeda, whose inspiration and motivation derive specifically from just such convictions. Moreover,**

these types of new regulations would contribute to the risk-averse environment that has been growing within the U.S. Intelligence Community since the Iraq War by discouraging NSA analysts from using the 702 program.

Recommendation 14 would extend the Privacy Act of 1974 in the same way to both U.S. persons and non-U.S. persons and calls for U.S. electronic surveillance to be guided by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. We reject this recommendation because it goes against the U.S. Constitution and U.S. security interests. The privacy and civil liberties of U.S. citizens and residents are protected by the U.S. Constitution. Those protections do not extend and should not be extended to non-U.S. persons abroad who have none of the duties and obligations of citizens and residents. This recommendation is extremely naïve and ignores the nature of intelligence: to break the laws of other states to obtain information to protect the security of our nation. Providing privacy rights to foreign persons would never be reciprocated and would shield American adversaries from U.S. intelligence agencies. It could also allow foreign persons to pursue legal action against the U.S. government.

Recommendation 15 would give NSA 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. **As discussed above, we reject this recommendation and propose replacing it with a similar proposal by the Senate Intelligence Committee in the FISA Improvements Act of 2013.**

Recommendations 19 and 21 address same concerns about foreign intelligence collection as recommendations 12, 13 and 14 and would put limits on intelligence collection against foreign persons in foreign countries. Recommendation 21 calls for the United States to enter into intelligence cooperation agreements with a small number of closely allied governments. **We reject recommendations 19 as a naïve throw-back to former Secretary of State Henry L. Stimson, who closed down a predecessor to the National Security Agency in 1929 because he believed "gentlemen don't read each other's mail." We are concerned that recommendation 21 could lead to too large an expansion of intelligence cooperation agreements, although we believe extending the "five-eyes" agreement to Germany and France should be studied.**

Recommendation 19 proposes to lay down criteria to limit surveillance against foreign leaders to ensure such collection is in the interests of the United States and will not have unnecessary negative effects on America's relations if such surveillance became known. **We reject this recommendation as an unnecessary proposal that runs counter to the nature of foreign intelligence collection and could discourage intelligence agencies from pursuing intelligence collection against foreign leaders who may be working against U.S. interests.**

3) Keep the U.S. Intelligence Collection Requirements Process Efficient and Effective

CSP's Recommendation

The process to approve intelligence collection requirements is already burdensome but generally effective. The Review Panel's recommendation to add additional layers of bureaucracy to this process and scores of policy officials would greatly slow down this process and create new security concerns. These recommendations would also make it more difficult to collect intelligence against foreign leaders which we believe would deny U.S. officials the crucial information they may need to make national security decisions. We urge that the U.S. intelligence collection requirements process be kept free of such new measures that would only bog it down, hampering its efficiency without providing any benefit.

The congressional intelligence committees were created to oversee and act as a check on intelligence activity by the Executive Branch that the American people would not support. To reassure the American people about sensitive intelligence collection programs, we believe steps should be taken to ensure that such collection efforts are always fully and promptly briefed to the oversight committees or congressional leaders as a way to win congressional buy-in for these programs in case something goes wrong.

The Review Group's Recommendations

Recommendations 16-18 would change who should direct the process of formulating, levying, and reviewing intelligence collection requirements, especially sensitive requirements and surveillance of foreign leaders. **We reject these recommendations because they ignore an existing collection framework that has proven to be effective, would bog down intelligence collection in new bureaucracy, and would pose security problems in protecting sensitive collection efforts.**

The Review Group ignores the existing legal framework that provides authority and direction for U.S. intelligence collection efforts, beginning with the National Security Act of 1947 and including the 1981 Executive Order 12333, the 1995 Presidential Decision Directive 35 (PDD-35), the Patriot Act of 2001 (as amended), the Intelligence Reform and Terrorism Prevention Act of 2004, and the National Security Presidential Directive-26 (NSPD-26). The Group takes special aim at the September 2007 National Intelligence Priorities Framework, a system of prioritized intelligence collection requirements, whose careful oversight procedures the Group explains before proceeding to recommend the imposition of an onerous new level of bureaucratic involvement "by all the departments and agencies with relevant concerns, including economic ones." The net effect of the Group's desired mandate that "any senior policymaker with relevant expertise and perspective" should be part of this process would amount to an unworkable burden of micromanagement and would raise security issues as it is unclear who these officials would be.

Recommendations 16, 17, and 18 propose the establishment of additional bureaucratic processes comprised of senior "policy and intelligence professionals" who would review intelligence collection requirements, apparently independently of already-established procedures under the purview of Congress and the National Security Council. **We reject these recommendations because they presume without any evidence that current intelligence collection approval**

procedures are inadequate for ensuring appropriate limits of "surveillance on foreign leaders and in foreign nations." Although the credentials and qualifications to be required of such "policy and intelligence professionals" are not discussed, the Group intends their focus to be the methods and targets of "sensitive" collection requirements out of concern that professional intelligence collection managers "may not always be aware that what they are doing or planning might fall into a category that makes it sensitive in the eyes of policymakers." A top concern of the Review Group would seem to be the embarrassment or other deleterious consequences that public disclosure of sensitive collection operations might cause to senior U.S. government policymakers and/or the economy of the U.S. It is the Group's conclusion that U.S. national security would be better served by constraining intelligence collection in order to ensure that there will never be any such embarrassment.

4) Support Intelligence Whistleblower Reform But Reject Duplicative Privacy Boards

CSP's Recommendation

We support modifications of Recommendation 27 to allow intelligence whistleblowers with privacy and civil liberty concerns to go directly to the Privacy and Civil Liberties Oversight Board as we believe this could serve as an additional safety valve for disgruntled intelligence employees to discourage them from leaking classified information to the news media and preventing future Snowdens.

The Review Group's Recommendations

Recommendations 25-28 would add additional layers of privacy and civil liberties protections and calls for Congress to create the position of Public Interest Advocate. **We oppose all of these recommendations except for a section dealing with intelligence whistleblowers. The Review Group's recommendations to add additional privacy officials are a solution in search of a problem and would overlap the existing Privacy and Civil Liberties Oversight Board. These provisions would also add a significant amount of new bureaucracy and regulations that will exacerbate the already cumbersome FISA Court process.**

In particular, with respect to the proposal for a Public Interest Advocate in the FISA Court, we note that preparing and submitting a FISA court application is already a cumbersome process, entailing the preparation of documents better measured in inches than in pages. To add another person who must review and prepare a response to such applications would add delay supported by no good reason. The Review Group acknowledges that judges already grant search warrants and wiretap orders in criminal investigations based on ex parte submissions from the government, and justifies its proposal only by claiming that the NSA program raises issues more complex than those involved in warrant applications. That claim has little basis in fact, and in any event takes no account of the oversight of intelligence activities by both senior executive officials and Congress – oversight that has no analogue in criminal investigations. We note that

the Senate Intelligence Committee's FISA Improvements Act of 2013 already has bipartisan language to enhance Privacy and Civil Liberties Oversight Board.

5) Make the NSA Director a Senate-Confirmed Position

CSP's Recommendation

Making the NSA Director a Senate-confirmed post is long overdue and will help restore public confidence to this post. We oppose the Review Group's other recommendations for NSA organizational reform as unnecessary steps that would interfere with NSA effectiveness.

The Review Group's Recommendations

Recommendations 22-24 concern organizational reforms and new oversight efforts supposedly to protect the privacy of Americans from NSA collection. We note that this series of recommendations arises from the following observation in the Review Group's report, which we quote in full:

> "After the terrorist acts in the United States of September 11, 2001, many people in both the Legislative and Executive Branches of government believed that substantial new measures were needed to protect our national security. We have noted that if a similar or worse incident or series of attacks were to occur in the future, many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy. The powerful existing and potential capabilities of our intelligence and law enforcement agencies might be unleashed without adequate controls. Once unleashed, it could be difficult to roll back these sacrifices of freedom."

In other words, the Review Group is animated by the belief that we should fear our fellow citizens more than we fear terrorists, and we should weaken our law enforcement and intelligence capabilities against the day when our fellow citizens try to "unleash" them. The Review Group's entire report should be viewed through the prism of that paragraph.

We oppose most of Recommendations 23 and 25-28 because they imply abuses by NSA that have not occurred and would create additional hoops for NSA to jump through to get approval for electronic surveillance.

Recommendation 22 would make the Director of the National Security Agency a Senate-confirmed position and allow civilians eligible to hold that position. It also calls for the President to give serious consideration to making the next Director of the National Security Agency a civilian. **We endorse both proposals because we believe they may help restore public confidence in NSA and NSA collection. Making the NSA Director Senate-confirmed would put pressure on the Senate Intelligence Committee to only confirm extremely well-qualified nominees and to prevent this post from being used for political patronage.**

Recommendation 23 calls for the National Security Agency to be clearly designated as a foreign intelligence organization; missions other than foreign intelligence collection should generally be reassigned elsewhere. **We oppose this recommendation as an unnecessary restriction on NSA in a world of rapidly changing communications technologies. Part of NSA's job is to detect transnational hostile intelligence and terrorist activity that threatens U.S. national security; inevitably, there will be American citizens found to be involved in such activity. While laws and directives governing NSA intelligence-gathering also specify policies and procedures to safeguard the constitutional rights of U.S. citizens, involvement with hostile foreign intelligence or terrorist organizations are not among those.**

Recommendation 24 would make the head of U.S. Cyber Command, and the Director of the National Security Agency separate officials. Recommendation 25 would move the NSA Information Assurance Directorate into the Department of Defense and report to the cyber policy element within the Office of the Secretary of Defense. **We oppose because these proposals are unnecessary and would restrict NSA's capabilities by putting these functions in a different organization.**

6) Keep Terrorist Communications and Software as Legitimate Targets for NSA

CSP's Recommendation

The Review Group's recommendations barring U.S. intelligence agencies from cracking internet encryption methods and penetrating computer software would seriously undermine critical intelligence collection by making the communications and software of terrorists and hostile powers off limits to NSA collection. We strongly urge that NSA be encouraged to continue doing what it does best: applying the best minds and latest technology to gaining technological access wherever needed in order to stay one step ahead of this country's adversaries.

Recommendation 35 calls for the U.S. government to develop privacy and civil liberties impact assessments for "big data" to ensure such efforts are statistically reliable, cost effective and protective of civil liberties. We reject this recommendation because it only focuses on privacy issues and ignores the enormous opportunities big data presents to produce valuable intelligence for policymakers and the complex challenges that big data intelligence efforts create for cooperation between telecommunications and internet companies and U.S. intelligence agencies. We therefore recommend a commission be formed to examine big data intelligence more broadly and prepare a report with recommendations for President Obama and Congress.

The Review Group's Recommendations

Recommendation 29 focuses on what the Review Group believes could be damage to open and secure global communications should the international community, and in particular, U.S. trading partners, become concerned about the security of U.S.-based information technology companies. To address this concern, the Review Group calls for the U.S. government to not undermine efforts to create encryption standards and not subvert, undermine, weaken, or make vulnerable generally available commercial software. It also makes an unobjectionable proposal to

increase the use of encryption and urges US companies to do so. **We reject this recommendation because it would effectively put the communications of U.S. enemies off-limits to U.S. intelligence agencies. We believe this recommendation reflects a naive view which ignores that we live in a world where the U.S. faces determined adversaries, including modern nation states as well as sub-national criminal and terrorist groups which are increasingly tech-savvy. Because of this reality, we believe the Internet and encryption deserve no special protections from legal and properly-monitored foreign intelligence collection programs.**

Recommendation 30 calls for the National Security Council staff to manage an interagency process to review on a regular basis the activities of the U.S. Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system known as "Zero Day" attacks. **Although we support the concept of protecting Americans by preventing Zero-Day attacks on U.S. computers, the text of this recommendation would allow NSA to exploit Zero–Day vulnerabilities against only under very narrow circumstances subject to enormous inter-agency review that would effectively remove this important weapon from NSA's arsenal. Similarly to recommendation 29, this would put software vulnerabilities of America's adversaries off limits to NSA. We reject this idea because the software of foreign persons outside the United States deserves no special protection from legal and properly-monitored foreign intelligence collection programs.**

Recommendations 34 and 36 aim to address civil liberty concerns related to cyber collection by U.S. intelligence agencies. **We reject these proposals as unnecessary and because they would attempts to bog down NSA cyber collection against foreign targets in bureaucracy due to unproven privacy concerns.**

7) Cyberwarfare Won't be Stopped by Treaties

CSP's Recommendation

The Review Group's proposal that all nations agree not to use surveillance to steal industry secrets or engage in cyberwarfare is unrealistic and will be disregarded by nations like China, Iran, North Korea, and Russia that engage regularly in this activity and will simply use the self-imposed restraint of others to their advantage. Moreover, it should be noted that U.S. law already prohibits U.S. intelligence collection for the benefit of private industry but cyberwarfare is and may be expected to remain one of the key battle spaces of coming decades. Voluntarily ceding such key territory to potential adversaries would be hugely detrimental to U.S. national security. Although we support the extensive international cooperation on matters concerning communications technology and regulation of the Internet that already exists, we believe that U.S. retention of a strong role in Internet governance remains in the best interests of national security.

The Review Group's Recommendations

Recommendation 31 calls for the United States to support and promote international norms or international agreements for specific measures that will increase confidence in the security of

online communications and calls on government not to "use surveillance to steal industry secrets to advantage their domestic industry." Recommendation 32 would create a new State Department Assistant Secretary for international information technology issues. Recommendation 33 would have the United States "advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments." **We oppose these Recommendations 31 and 32 because they represent pointless diplomacy to get agreements that Western governments might abide by but hostile powers will ignore. We oppose Recommendation 33 since although the Review Group says it does not advocate transferring control of the Internet to UN organizations, this proposal is a move in this direction.**

8) Urgent Reforms Needed in Security Clearances and Protecting Classified Computer Networks

CSP's Recommendation

Urgent reforms are needed to improve the process for obtaining and renewing security clearances and the security of computer networks. We believe the problem with security background investigations is not that they are outsourced, but rather that this process has been poorly managed by government officials who have prioritized volume and speed with which clearances are processed rather than the quality of these investigations. We believe this has nothing to do with for-profit vs nonprofit companies -- either can do the job so long as they are highly qualified, have clear contract performance criteria, and are subject to proper oversight by the government, including high standards for training investigators. We believe a bigger issue is the enormous number of U.S. clearance holders which has expanded to some 5 million people.

The Review Group's Recommendations

In response to a weak security clearance vetting process that allowed Edward Snowden to obtain numerous high level clearances to work for an intelligence contractor, Recommendations 37-46 address the urgent need to improve the security clearance process and the security of classified computer networks to prevent another Snowden incident. **We support most of these proposals in principle but call for them to be further studied by an intelligence clearance taskforce.**

Recommendation 37 calls for the U.S. Government moving toward a system in which background investigations on the vetting of personnel for security clearances are performed solely by U.S. Government employees or by a non-profit, private sector corporation. Recommendation 38 calls for the vetting of personnel for access to classified information to be ongoing, rather than periodic. **We reject these proposals because we believe they are impractical, although we agree with their intent.** Background investigations have been outsourced because the government doesn't have enough employee-investigators; if they were all brought in-house, the backlogs would be staggering. This would mean longer times between re-investigations, thus creating a new security vulnerability. The idea of ongoing security vetting of millions of clearance holders is probably impossible to implement and could pose troubling civil liberties implications.

Recommendation 39 calls for security clearances to 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. **We support this recommendation and believe any differentiation should be part of a broader review of which positions need access to what level of material.**

Recommendation 40 calls for 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. **We reject this recommendation because it is unclear what it would accomplish.**

Recommendation 41 calls for "need-to-share" or "need-to-know" models 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. **We support this recommendation but recommend that we return to the "need to know" standard.**