NATIONAL SECURITY AND OPEN GOVERNMENT pdf

1: Classified information in the United States - Wikipedia

on National Security and Open Government held in Washington, DC on May 5, The symposium was a jointly run project of the Campbell national security.

Samantha Power on transparency, national security and open government How open government can have a global impact. The issues created between Wikileaks and open government policies are substantial. Open data may be used for accountability, citizen utility and economic opportunity. The keynote talk and discussion with Samantha Power, special assistant to the President for multilateral affairs and human rights, and member of the National Security Council, was designated as off-the-record by conference organizers. No livestream, no tweets, no liveblogging. The situation resulted, however, not from any policy decision but simply from the press office running behind during a long trip abroad, said White House National Security Council spokesman Bob Jensen. This stuff happens all the time. Looking back, Power said that none of the comments she made to the open government data conference should be considered sensitive. Power discussed her experience using Data. She highlighted how technology has changed the ways that citizens around the world can share information about government performance, access economic information, or share key health indicators, including several of the initiatives that she saw when she traveled with President Obama to India. Power subsequently blogged at WhiteHouse. What follows is our interview, edited for both clarity and length. How do you balance national security concerns with open government? There are two factors that are always brought to bear in discussions in open government , as President Obama has made clear from the day he issued his memorandum. One is privacy, one is security. There are also, of course, reasons to protect the deliberative process. He addressed some of this in his speech at the National Archives. Can that be changed by open government initiatives? I think transparency can get at a number of different issues at once. Data, transparency, and access to information are also being used in ways that enhance citizen welfare. If you put toy recall data up online, or look at OSHA data â€" these are ways of providing to citizens information that government has long collected. Government is an incredible information collecting machine. I see a change happening in rules. The public comments on regulations are pored over by officials in the domestic space; as a result, rules are changed and much improved. Some of the trust deficit involves specific policies that people are determined to see delivered on. To the degree that there are people of good will who are willing to sit down and have discussions about open government and transparency, those can have good effect. Consider the Indian examples from the expo. Which tools are you excited about, specifically? Each government, and, hopefully, civil society, will come together. Brazil, I think, has been a real leader in participatory budget processes. Indonesia has done a lot to root out police corruption. Citizens can file â€" and governments can respond â€" to complaints lodged online. Indians have a strong right to information law. One thing I do want to stress: As we embark on a global open government initiative, we want to do so partnering with a very diverse group of countries by our side. How can open government, transparency or technology address human rights issues? No one reifies technology for its own sake. What was really exciting in India was that the President got to touch and feel technology being used for to promote democratic progress and accountability. Technology was being used by citizens that had been disempowered, disenfranchised. Suddenly, with connection they could be be empowered, and their voices included in discussions. Technology is neither necessary for open government nor sufficient. And of course, on occasion, technology can also be harnessed in ways that can be antithetical to basic human rights. In Indonesia, we celebrated what Indonesian citizens are doing to hold government accountable and build democracy in the region. The convening power of the President of the United States can be used to partner with others to create a process through which they can make commitments to harnessing technology, fighting corruption, and collaborating more with their citizens to improve service delivery and increase democratic accountability. I think that this open government initiative is the kind of thing that, as it gets more traction, will get more public support.

NATIONAL SECURITY AND OPEN GOVERNMENT pdf

2: Samantha Power on transparency, national security and open government - O'Reilly Radar

NATIONAL SECURITY AND OPEN GOVERNMENT: STRIKING THE RIGHT BALANCE Campbell Public Affairs Institute The Maxwell School of Syracuse University Commentaries edited by the Campbell Public Affairs Institute from a.

Military security In practice, national security is associated primarily with managing physical threats and with the military capabilities used for doing so. Most states, such as South Africa and Sweden, [14] [10] configure their military forces mainly for territorial defence; others, such as France, Russia, the UK and the US, [15] [16] [11] [12] invest in higher-cost expeditionary capabilities , which allow their armed forces to project power and sustain military operations abroad. Economic security Economic security, in the context of international relations , is the ability of a nation state to maintain and develop the national economy, without which other dimensions of national security cannot be managed. In larger countries, strategies for economic security expect to access resources and markets in other countries, and to protect their own markets at home. Developing countries may be less secure than economically advanced states due to high rates of unemployment and underpaid work. Environmental security Ecological security, also known as environmental security, refers to the integrity of ecosystems and the biosphere , particularly in relation to their capacity to sustain a diversity of life-forms including human life. The security of ecosystems has attracted greater attention as the impact of ecological damage by humans has grown. The scope and nature of environmental threats to national security and strategies to engage them are a subject of debate. These include global environmental problems such as climate change due to global warming , deforestation , and loss of biodiversity. These include resource scarcities leading to local conflict, such as disputes over water scarcity in the Middle East ; migration into the United States caused by the failure of agriculture in Mexico ; [1]: These include acts of war that degrade or destroy ecosystems. Energy security Resources include water, sources of energy, land and minerals. Availability of adequate natural resources is important for a nation to develop its industry and economic power. For example, in the Persian Gulf War of , Iraq captured Kuwait partly in order to secure access to its oil wells, and one reason for the US counter-invasion was the value of the same wells to its own economy. The interrelations between security, energy, natural resources, and their sustainability is increasingly acknowledged in national security strategies and resource security is now included among the UN Sustainable Development Goals. Computer security Computer security , also known as cybersecurity or IT security, refers to the security of computing devices such as computers and smartphones, as well as computer networks such as private and public networks, and the Internet. It concerns the protection of hardware, software, data, people, and also the procedures by which systems are accessed, and the field has growing importance due to the increasing reliance on computer systems in most societies. Infrastructure security seeks to limit vulnerability of these structures and systems to sabotage , terrorism , and contamination. There are also commercial transportation security units such as the Amtrak Police in the United States. Critical infrastructure is vital for the essential functioning of a country. Incidental or deliberate damage can have a serious impact on the economy and essential services. Some of the threats to infrastructure include: In the November Mumbai attacks , the Mumbai central station and hospital were deliberately targeted, for example. Cyberattacks on Estonia and cyberattacks during the South Ossetia war are examples. Issues in national security[edit] Consistency of approach[edit] The dimensions of national security outlined above are frequently in tension with one another. The high cost of maintaining large military forces places a burden on the economic security of a nation. Unilateral security action by states can undermine political security at an international level if it erodes the rule of law and undermines the authority of international institutions. The invasion of Iraq in and the annexation of Crimea in have been cited as examples. If tensions such as these are not managed effectively, national security policies and actions may be ineffective or counterproductive. National versus transnational security[edit] Increasingly, national security strategies have begun to recognise that nations cannot provide for their own security without also developing the security of their regional and international context. Some argue that the principal beneficiary of national security policy should be the nation

state itself, which should centre its strategy on protective and coercive capabilities in order to safeguard itself in a hostile environment and potentially to project that power into its environment, and dominate it to the point of strategic supremacy. For example, the rights and liberties of citizens are affected by the use of military personnel and militarised police forces to control public behaviour; the use of surveillance including mass surveillance in cyberspace ; military recruitment and conscription practices; and the effects of warfare on civilians and civil infrastructure. This has led to a dialectical struggle, particularly in liberal democracies , between government authority and the rights and freedoms of the general public. The National Security Agency harvests personal data across the internet. Even where the exercise of national security is subject to good governance and the rule of law , a risk remains that the term national security may be become a pretext for suppressing unfavorable political and social views. In the US, for example, the controversial USA Patriot Act of , and the revelation by Edward Snowden in that the National Security Agency harvests the personal data of the general public , brought these issues to wide public attention. Among the questions raised are whether and how national security considerations at times of war should lead to the suppression of individual rights and freedoms, and whether such restrictions are necessary when a state is not at war.

NATIONAL SECURITY AND OPEN GOVERNMENT pdf

3: Transparency and Open Government | www.enganchecubano.com

Abstract. There are circumstances in which governments can legitimately restrict openness in the name of national security. However, we can identify three common problems that arise when governments invoke national security concerns to restrict transparency.

For questions, contact blog cagw. October 25, - Open source code allows anyone to easily inspect, modify, and enhance an IT system since it is accessible to the general public. However, in February , DOD began experimenting with open source code, although the practice has not been adopted department-wide. The recent Equifax breach highlights the dangers of open source software. On September 7, , Equifax announced a cybersecurity hack had occurred to its open source system Adobe Struts between May and July , in which the personal identification information of roughly million people was extracted. Making public the source code to a centralized software network not only unlocks the door for attackers, but also makes it very difficult for a company to account for problems within complex systems, especially when there are thousands of open source components developers must sift through and integrate. In addition, companies using open source products often have difficulty in properly monitoring changes and modifications to the software, and therefore are ill-prepared to divert a potential attack. Once weaknesses are found, hackers can exploit them over and over again on the dark web. In addition to the national security risks, these NDAA provisions threaten intellectual property and have the potential to stifle innovation and competition. As currently written, Section violates U. Such drastic steps could results in grave consequences for the innovation economy. Asking tech companies to turn over their source code to the government decreases competition and gives them less of a reason to innovate. It is simply not credible to believe that this fledgling operation with approximately employees scattered throughout the U. Congress should not effectively close DOD to any software option that might better serve taxpayers. Although most of these provisions are limited to the DOD, Section sets a precedent that could establish open source as the preferred method for software procurement throughout the government. That would reverse the July 1, Office of Management and Budget software acquisition memorandum which requires federal software purchases to be technology neutral. This potential snowball effect could expose the government to the risk of greater cybersecurity attacks and impinge on the intellectual property rights of technology companies that contract with the federal government. The federal government should quickly learn from high-profile incidents like the Equifax breach, which demonstrates that even the private sector has difficulty managing and protecting open source code. Beyond the inherent issue of government mandating technology solutions, requiring the DOD to begin using open source code as its preferred software solution is a risk to national security and intellectual property that simply cannot be made. The Council for Citizens Against Government Waste, along with nine other organizations, has urged the NDAA conferees to remove these problematic provisions in order to prevent potentially disastrous results.

4: The White House | www.enganchecubano.com

national security, including non-governmental organizations, academics, and members of government. The aim of the meeting was to discuss how national security is impacting on the rights to freedom of expression and information at the beginning of the 21st Century.

It covers records that are: A specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy and B are in fact properly classified pursuant to such an executive order. In , President Bill Clinton issued an executive order intended to limit the circumstances under which government agencies can classify information and to hasten the declassification of records for which classification has become unnecessary after the passage of time or a change in circumstances. The Bush order also called for automatic classification of foreign government information when disclosure is not authorized, under a presumption that disclosure would damage national security. If the records you seek do not fit into any of the categories, they should not have been classified at all. Records that are classifiable concern military plans, weapons or operations; foreign government information; intelligence sources, methods or cryptology; scientific, technological or economic matters relating to national security; U. The government must justify the withholding of each document, and within each document it must justify the withholding of every paragraph, sentence, word and phrase. Just because information is in the possession of the Central Intelligence Agency or the Department of Defense or Department of State does not necessarily mean it is classified. In , the U. District Court in Manhattan held that Exemption 1 protected past and present photographs of inmates housed at the military base at Guantanamo Bay, Cuba, because of the safety risks to the detainees and their families from terrorist organizations. This information may still, in many cases, be released via a FOIA request. If your FOIA request is denied and you ultimately file a lawsuit, the agency will submit affidavits to the court explaining the nature of the withheld information and that it is classified. The courts often give substantial deference to these affidavits. In these cases, the suit may be dismissed at an early stage. Sometimes judicial inspection can be helpful in securing access to historical records that were obviously classified merely to prevent political repercussions. Agencies might avoid a decision on the release of classified records if the fact the records even exist is itself classifiable. In a FOIA case involving a request for records pertaining to a ship, the Glomar Explorer, an appeals court allowed the CIA to neither confirm nor deny the existence of the requested records. When agencies neither confirm nor deny the existence of records, requesters should not presume that the records exist. Unfortunately, agencies are also using the Glomar response while invoking the privacy exemptions as well the exemption for national security. For the requester who seeks classified records, the most important question is whether to file a FOIA request at all. Under the Bush executive order, a requester can seek mandatory declassification review rather than file a FOIA request. However, unlike denial of a FOIA request, a denial of mandatory declassification review request cannot be appealed to a court. Also, under mandatory declassification review, reviewers have a longer time to inspect records and do not have to abide by expedited processing requirements, but the requester does not have to pay fees as with FOIA. Typically, the mandatory declassification review process is better suited to processing requests for specifically identifiable documents that the requester knows are classified. In contrast, the FOIA process is better suited to handle requests for large amounts of information or for more general requests. Regulations to implement the Bush executive order require a requester to decide between FOIA and mandatory declassification review up front. The requester may not make a FOIA request and seek declassification review for the same classified records. Faced with a request for both, an agency will require the requester to elect one process or the other. If the requester fails to choose, the agency will treat the request as a FOIA request. If the requester simply seeks the information without mentioning either FOIA or mandatory declassification review, the agency will probably categorize the request as a FOIA request. Central Intelligence Agency, F.

NATIONAL SECURITY AND OPEN GOVERNMENT pdf

5: National security | Reporters Committee for Freedom of the Press

*National Security and Open Government: Striking the Right Balance [Campbell Public Affairs Institute] on www.enganchecubano.com *FREE* shipping on qualifying offers.*

Confidential, Secret, or Top Secret. Information that is not so labeled is called "Unclassified information". The term declassified is used for information that has had its classification removed, and downgraded refers to information that has been assigned a lower classification level but is still classified. Many documents are automatically downgraded and then declassified after some number of years. Reasons for such restrictions can include export controls , privacy regulations, court orders, and ongoing criminal investigations, as well as national security. Information that was never classified is sometimes referred to as "open source" by those who work in classified activities. Government produces more classified information than unclassified information. Having Top Secret clearance does not allow one to view all Top Secret documents. The user of the information must possess the clearance necessary for the sensitivity of the information, as well as a legitimate need to obtain the information. For example, all US military pilots are required to obtain at least a Secret clearance, but they may only access documents directly related to their orders. Secret information might have additional access controls that could prevent someone with a Top Secret clearance from seeing it. Typically each president will issue a new executive order, either tightening classification or loosening it. The Clinton administration made a major change in the classification system by issuing an executive order that for the first time required all classified documents to be declassified after 25 years unless they were reviewed by the agency that created the information and determined to require continuing classification. These are the only two classifications that are established by federal law, being defined by the Atomic Energy Act of Nuclear information is not automatically declassified after 25 years. Documents with nuclear information covered under the Atomic Energy Act will be marked with a classification level confidential, secret or top secret and a restricted data or formerly restricted data marking. Nuclear information as specified in the act may inadvertently appear in unclassified documents and must be reclassified when discovered. Even documents created by private individuals have been seized for containing nuclear information and classified. Only the Department of Energy may declassify nuclear information. However some information is compartmentalized by adding a code word so that only those who have been cleared for each code word can see it. Each code word deals with a different kind of information. The CIA administers code word clearances. The classification of individual paragraphs and reference titles is shown in parentesesâ€”there are six different levels on this page alone. Notations with leader lines at top and bottom cite statutory authority for not declassifying certain sections. The highest security classification. Information is classified Secret when its unauthorized disclosure would cause "serious damage" to national security. Confidential[edit] This is the lowest classification level of information obtained by the government. It is defined as information that would "damage" national security if publicly disclosed, again, without the proper authorization. Certain positions which require access to sensitive information, but not information which is classified, must obtain this designation through a background check. Public Trust Positions can either be moderate-risk or high-risk. For example, the law enforcement bulletins reported by the U. This information is supposed to be released only to law enforcement agencies sheriff, police, etc. In addition to FOUO information, information can be categorized according to its availability to be distributed e. Department of Defense contractor personnel [22]. Documents subject to export controls have a specific warning to that effect. Information which is "personally identifiable" is governed by the Privacy Act of and is also subject to strict controls regardless of its level of classification. Finally, information at one level of classification may be "upgraded by aggregation" to a higher level. For example, a specific technical capability of a weapons system might be classified Secret, but the aggregation of all technical capabilities of the system into a single document could be deemed Top Secret. Use of information restrictions outside the classification system is growing in the U. In September J. William Leonard, director of the U. National Archives Information Security Oversight Office , was quoted in the press as saying, "No one individual in government can identify all the controlled, unclassified [categories], let alone describe their rules. Bush issued

a Presidential memorandum on May 9, , in an attempt to consolidate the various designations in use into a new category known as Controlled Unclassified Information CUI. The CUI categories and subcategories were hoped to serve as the exclusive designations for identifying unclassified information throughout the executive branch not covered by Executive Order or the Atomic Energy Act of as amended but still required safeguarding or dissemination controls, pursuant to and consistent with any applicable laws, regulations, and government-wide policies in place at the time. Congress has attempted to take steps to resolve this, but did not succeed. Because no action was taken in committee [29] and bills expire at the end of every Congress, there is currently no bill to solve unclassified designations. Classified classifications[edit] Executive Order , which forms the legal basis for the U. However, this executive order provides for special access programs that further restricted access to a small number of individuals and permit additional security measures Sec. These practices can be compared with and may have inspired the concepts multilevel security and role-based access control. Proper procedure for classifying U. A determination must be made as to how and when the document will be declassified, and the document marked accordingly. Executive Order describes the reasons and requirements for information to be classified and declassified Part 1. Individual agencies within the government develop guidelines for what information is classified and at what level. The former decision is original classification. A great majority of classified documents are created by derivative classification. For example, if one piece of information, taken from a secret document, is put into a document along with pages of unclassified information, the document, as a whole, will be secret. Therefore, in this example, only one paragraph will have the S marking. If the page containing that paragraph is double-sided, the page should be marked SECRET on top and bottom of both sides. Many interpretations exist concerning what constitutes harm or the degree of harm that might result from improper disclosure of the information, often leading to inconsistent or contradictory guidelines from different agencies. There is wide variance in application of classification levels. Current policy requires that the classifier be "able" to describe the basis for classification but not that he or she in fact do so. Classification categories are marked by the number "1. Classifying non-government-generated information[edit] The Invention Secrecy Act of allows the suppression of patents for a limited time for inventions that threaten national security. Whether information related to nuclear weapons can constitutionally be " born secret " as provided for by the Atomic Energy Act of has not been tested in the courts. Guantanamo Bay detention camp has used a "presumptive classification" system to describe the statements of Guantanamo Bay detainees as classified. Protecting classified information[edit] GSA-approved security container Facilities and handling[edit] One of the reasons for classifying state secrets into sensitivity levels is to tailor the risk to the level of protection. The rooms or buildings for holding and handling classified material must have a facility clearance at the same level as the most sensitive material to be handled. Good quality commercial physical security standards generally suffice for lower levels of classification; at the highest levels, people sometimes must work in rooms designed like bank vaults see Sensitive Compartmented Information Facility â€” SCIF. Congress has such facilities inside the Capitol Building , among other Congressional handling procedures for protecting confidentiality. General Services Administration sets standards for locks and containers used to store classified material. The most commonly-approved security containers resemble heavy-duty file cabinets with a combination lock in the middle of one drawer. In response to advances in methods to defeat mechanical combination locks, the U. After a specific number of failed attempts, they will permanently lock, requiring a locksmith to reset them. Authors must mark each paragraph, title and caption in a document with the highest level of information it contains, usually by placing appropriate initials in parentheses at the beginning of the paragraph, title, or caption. Commonly, one must affix a brightly colored cover sheet to the cover of each classified document to prevent unauthorized observation of classified material shoulder surfing and to remind users to lock up unattended documents. The most sensitive material requires two-person integrity , where two cleared individuals are responsible for the material at all times. Approved containers for such material have two separate combination locks, both of which must be opened to access the contents. Top Secret material must go by special courier; Secret material within the U. CCI equipment and keying material must be controlled and stored with heightened physical security, even when the device is not processing classified information or contains no cryptographic key. Suite B provides

protection for data up to Top Secret on non-CCI devices, which is especially useful in high risk environments or operations needed to prevent Suite A compromise. These less stringent hardware requirements stem from the device not having to "protect" classified Suite A algorithms. These systems enforce the classification and labeling rules described above in software. Since , however, they are not considered secure enough to allow uncleared users to share computers with classified activities. Thus, if one creates an unclassified document on a secret device, the resultant data is classified secret until it can be manually reviewed. The destruction of certain types of classified documents requires burning, shredding , pulping or pulverizing using approved procedures and must be witnessed and logged. Lifetime commitment[edit] When a cleared individual leaves the job or employer for which they were granted access to classified information, they are formally debriefed from the program. Debriefing is an administrative process that accomplishes two main goals: Typically, the individual is asked to sign another non-disclosure agreement NDA , similar to that which they signed when initially briefed, and this document serves as the formal record. The debriefed individual does not lose their security clearance ; they have only surrendered the need to know for information related to that particular job. Classifications and clearances between U. Casey for Secret info showing up in The New York Times , but then saying it was over-classified to begin with. For example, an individual cleared for Department of Defense Top Secret had to undergo another investigation before being granted a Department of Energy Q clearance. Agencies are now supposed to honor background investigations by other agencies if they are still current. For example, officials visiting at the White House from other government agencies would pass their clearances to the Executive Office of the President EOP. At one time, a person might hold both a TS and a Q clearance, but that duplication and cost is no longer required. Contrary to popular lore, the Yankee White clearance given to personnel who work directly with the President is not a classification. Individuals having Yankee White clearances undergo extensive background investigations. The criteria include U. Some compartments, especially intelligence-related, may require a polygraph examination, although the reliability of the polygraph is controversial.

6: national security and open government | Download eBook pdf, epub, tuebl, mobi

There are circumstances in which governments can legitimately restrict openness in the name of national security. However, we can identify three common problems that arise when governments invoke.

7: National security - Wikipedia

Beyond the inherent issue of government mandating technology solutions, requiring the DOD to begin using open source code as its preferred software solution is a risk to national security and intellectual property that simply cannot be made.

8: National Security and Open Government | red file

Ministers from various government departments are allowed to refuse to provide information if they believe that "the information constitutes special operation information, as defined in the subsection 8(1) of the Security of Information Act; and provision of the information would be injurious to national security.".

9: Securing an Open Society: Canada's National Security Policy

The publication of the National Security Strategy (NSS) is a milestone for any presidency. A statutorily mandated document, the NSS explains to the American people, U.S. allies and partners, and.

NATIONAL SECURITY AND OPEN GOVERNMENT pdf

The artist and the changing garden Betsy G. Fryberger V.2. Industrial art, by Prof. Walter Smith. The Wrath of Dionysus Wittgenstein-Aesthetics and Transcendental Philosophy (Schriftenreihe der Wittgenstein-Gesellschaft) Basket ball for women The fertilizer encyclopedia Secrets of Chess Training Postscript : How rude are we? Savannahs Amanda Barrett. Windows explorer 10 preview Bermuda triangle book in urdu Fill out for Lined paper with margin Montana Sky (Heartsong Presents #161) Umrah guide book in english Reach, touch, and teach Formation of econometrics Group Psychotherapy for Women With Breast Cancer Valentine Sampler 3. Special Status States (Arts. 370 371) Telluride, Pandora the Mines Above Bmw z3 2.8 manual Tricks of the Windows 3.1 masters Nomination of Sylvia M. Mathews The twelve tones of the spirit. The 13 secrets of power performance The medieval idea of the Bible Stage-Land (Dodo Press) The mirror with a memory chapter 9 2006 Scott US Specialized Valuing Supplement Not-knowing Donald Barthelme The autobiography of a new england farm house P. 2. Production versions. Framework components Legends of Jerusalem (Sacred Land, Vol 1) Trucks and construction Industrial Applications of Semantic Web Music education in the United States Housekeeping supervision. The Eternal Mystery