OPEN SOCIETY FOUNDATIONS

OPEN GOVERNMENT PARTNERSHIP SECURITY SECTOR SAMPLE COMMITMENTS

September 2011

To help inform governments, civil society and the private sector in developing their OGP commitments, the Transparency and Accountability Initiative (T/A Initiative) reached out to leading experts across a wide range of open government fields to gather their input on current best practices and the practical steps that OGP participants and other governments could take to achieve meaningful progress.

The Open Society Foundations drafted three sets of sample commitments, in consultation with partners around the world, that recommend concrete steps to address aspects of one of the five "grand challenges" identified by the OGP Steering Committee as foundational, namely:

> Creating Safer Communities—measures that address public safety, the security sector, disaster and crisis response, and environmental threats.

The below sample commitments address transparency and accountability concerning:

- Police and Public Security,
- Military and Intelligence Budgets, and
- National Security.

Police and Public Security[1]

I. Initial Steps

Across the globe, the primary point of contact most citizens have with their government is a police officer. Competent and honest law enforcement is a mainstay of the rule of law. Insufficient or ineffective investment in the public security sector can result in weak or non-functioning security institutions, unable to respond to, or deter, crime and violence.

Goal: States make information on budgets, personnel and crime publicly available in a timely and accessible manner.

Justification: Basic information on budgets, line accountability and crime rates is necessary for citizens to assess the costs of policing and distribution of law enforcement resources relative to public safety needs as well as to other spending priorities.[2]

Recommendations:

1. States should publish all laws and regulations setting out police powers (including regulations concerning the private security sectors).
2. States should publish basic budgets and lines of leadership and authority for national police force(s).
3. States should publish basic data on number of personnel (distinguishing sworn officers and administrative staff); number of police officers per capita and by region; names and functions of special units; numbers of officers assigned to each special unit; and weapons and non-lethal equipment assigned to officers.
4. States should publish the number of recorded crimes, breaking out violent crime from property crime, and within violent crime, noting numbers of homicides and rapes and other gender violence.
5. States should publish the arrest rate and clearance rate (rate of handling cases) on an ongoing basis and in a timely and accessible manner.
6. States should provide information to citizens on how to register a complaint against the police (including where and how to file a complaint, protection for whistleblowers, the process for reviewing complaints, time-frames for adjudication).

[1] OSF thanks Prof. David Bayley, State University of New York at Albany, and Prof. Hugo Frühling, University of Chile, and Director of the Center for Studies on Public Safety, for their comments

[2] Countries organize their police systems in different ways. Most of them have more than one police force—e.g., state police, communal police, municipal police, and/or judicial police. Some also undertake military duties (e.g., gendarmerie), and in some countries military forces supplement police forces in national emergencies (Mexico, Egypt) and/or to help carry out basic police functions (Nigeria). There may also be special police forces or units (e.g. tax and military police). In some countries, the main forces operate at the state and local levels, and national police forces specialize in addressing particular categories of crime (e.g., drug enforcement, immigration and customs enforcement).

II. More Substantial Steps

Goal: States disclose more detailed information about budget allocations; cases of misconduct and complaints against police; information about the actors involved in protecting citizens; and disaggregated information on patterns of criminality and justice.

Justification: Publication of information—about the structures and numbers of police personnel, salary scales, seized assets, persons in detention, and measures of core activities of the criminal justice system—is one of the most powerful ways to protect against corruption and mismanagement in police forces, support more informed discussion of operational approaches, and improve public perception of the police. Care, however, must be taken to avoid perverse incentives, a risk especially when activity measures are set as key performance indicators. Information about patterns of criminality, including distribution and level and rates of crime, allow citizens to assess whether remedial approaches being taken are effective and whether the police are addressing crimes that affect most people, or targeting special interests or groups to their advantage or disadvantage. For instance, if a country's budget is published revealing high amounts for the police relative to other essential functions, and the numbers of crimes recorded and arrests made are relatively low, then the public is better positioned to raise questions about efficiency and good management, and assess whether the information suggests good policy or, to the contrary, mismanagement and corruption.

Recommendations:

1. States should publish information on lines of authority and chains of command so that responsibility is clear.
2. All police personnel–including senior management, district and regional chiefs and patrol officers–should be publicly identifiable (that is, they should be required to wear badges with names or ID numbers clearly visible).
3. Private security personnel should also be clearly identifiable by company name and badge number or name.
4. Basic pay scales, qualifications for entry to the police, recruitment and promotions processes should be public.
5. Data about assets seized by the police (including real estate, cars, weapons, drugs, and cash) should be made public on an ongoing basis, in a timely and accessible manner.
6. States should publish data on complaints against police, both those received directly by police and those made to prosecutors, independent complaint bodies and ombudsmen offices, including reasons for those complaints and their disposition (including rejected, substantiated, mediated, upheld) and all disciplinary actions taken against officers.
7. States should publish information on procurement rules, regulations and procedures. All tenders and major acquisitions should be public, as well as the names of companies winning contracts.
8. Crime data should be further disaggregated by age, sex, ethnic background or nationality, weapon used if any, and region.

9. States should publish data on persons held in police detention, including length of detention, age, sex, ethnic background and nationality, and geographic district.

III. Most Ambitious Steps

Goal: States publish national crime statistics and submit datasets and other information to international bodies so that progress can be tracked over time. Information is generated that enables scrutiny of each stage of the criminal justice system from police, prosecutors, courts, corrections and probation departments, as well as coordination among the various stages.

Justification: Timely information about national crime statistics is essential in order to be able to track and address overall trends and sub-trends, and compare criminal patterns across countries. Criminal justice systems include many components that do not work independently and problems frequently arise concerning coordination between various steps of the criminal justice process. Information that tracks the progress of individuals through the criminal justice system is important both to detect and address abuse and corruption and to support development of fairer and more effective policies.

Recommendations:

1. States should compile and publish annual victimization surveys/crime reports so that overall trends and sub-trends can be monitored.[3]
2. States should submit data to the UN Office on Drugs and Crime for the International Crime and Victimization Survey.[4]
3. States should publish data on the number of people in pre-trial detention, acquitted, and serving sentences in prison.
4. States should make national crime data bases (including victimization surveys) open and accessible to academic researchers and civil society organizations and the general public, and further publication should be permitted without restrictions.
5. Information should also be disclosed in a systematic fashion on-line and made available locally through media and posting at police stations.
6. Data sets should be available online in formats that are easily downloadable in order to facilitate comparison with other government data sets.

7. States should collect and publish detailed information on criminal justice statistics from policing through to probation, including the following:
    - *Police data*. Basic demographic statistics on the police force and administrative staff, including sex, age group, and ethnic background or nationality.
    - *Prosecution statistics*. Data covering all steps of decision-making by prosecutors, including initiating and abandoning prosecutions, bringing cases to court, and sanctioning offenders by summary decisions.

[3] See, e.g., the US Annual Crime report produced by the FBI, and the annual British Crime Survey published by the UK Home Office, http://rds.homeoffice.gov.uk/rds/bcs1.html.
[4] UNODC crime and criminal justice statistics, http://www.unodc.org/unodc/en/data-and-analysis/crimedata.html.

- *Detention statistics.* Regular data on persons in police custody, in pre-trial detention, and on bail and electronic monitoring, including the legal bases (charges) and length of detention.
- *Judicial (Court) statistics*. Integrated systems of data related to all actors in the criminal justice system.
- *Conviction statistics*. Data on persons who have been convicted—i.e., found guilty according to law – disaggregated by offence and by sex, age group, and ethnic background or nationality of the offender. [5]
- *Corrections.* Information on numbers of persons in detention, distinguishing juveniles and women, and type of facility (e.g., high, medium or minimum security), early release decisions, and numbers of persons on probation. Figures should enable analysis of repeat offending and cycling through the criminal justice system.

Military and Intelligence Budgets

National governments expend from 2 to 8 percent of gross domestic product (GDP) and 2 to 30 percent of central government expenditure (CGE) on the military sector—with the global average hovering at 11 percent of CGE since 2002.[6] The IMF has found that higher levels of military spending (as a percentage of GDP or CGE) correlate positively with corruption, and higher levels of weapons procurement correlate most markedly with corruption.[7]

Access to reliable and relevant data on military expenditure can not only help expose and deter corruption, but also allows scholars and the public to assess and seek to influence a government's priorities and track changes in the relative level of military expenditure over time, which may indicate how a particular state views its security threats. For instance, rapid increases in military expenditure over a short period of time may be a warning sign of imminent internal or external conflict.

During the Cold War, governments on both sides accommodated some transparency in military spending without apparently compromising their security. Since the end of the East-West divide, the international community has sought to increase openness in the security sector in all regions of the globe in order to build internal and international trust. Even in the area of intelligence budgeting, the part of the security sector that remains most firmly in the dark, several governments have increased openness in recent years without any harm to their national security as a result.

I. Initial Steps

[5] See, e.g., European Sourcebook of Crime and Criminal Justice Statistics, fourth edition, 2010, http://www.europeansourcebook.org/ob285_full.pdf.
[6] World Bank, World Development Indicators, http://data.worldbank.org/indicator/MS.MIL.XPND.ZS (based on SiPRI Milex data).
[7] Gupta, Sanjeev et al., "Corruption and Military Spending," IMF, Fiscal Affairs Department, February 2000, p. 16.

Goal: Governments make accurate information about military spending publicly available in a reasonably detailed and disaggregated form.[8]

Justification: The more detailed the information made available to the public, the more protection there is against misuse of funds and the greater is the potential for building trust within and across borders.

Recommendations:

1. Governments annually publish military budgets, including a breakdown of figures for personnel (disaggregated), procurement, research and development (if applicable), construction, and operations. Information should be included about off-budget expenditure and revenue sources for the military (e.g., industries or natural resource concessions under the control of the armed forces) and foreign assistance flowing directly to defense/security budget lines.
2. Governments specify whether paramilitary forces exist and, if so, whether they are included in the military budget.
3. Governments submit reasonably detailed data to the United Nations via the Standardized Instrument for Reporting Military Expenditures (MilEx).[9]

Country Examples: The great majority of the world's countries provide some basic data on military expenditure, in many cases over the Internet as well as in printed official documents.[10] But comprehensiveness, accuracy, detail and accessibility are lacking for most. UN member states agreed to begin submitting data on their military expenditure to the United Nations in 1981. In 2009 and 2010, 20 countries submitted information via a simplified form--including Armenia, Cambodia, El Salvador, Indonesia, Israel, and Lebanon, and another 40 provided data using a more detailed form, including Burkina Faso, Colombia, and Nepal.

II. More Substantial Steps

Goal: Transparency, accountability, and oversight procedures that permit citizen engagement in all stages of military budgeting, spending, procurement, and auditing.

Justification: A more open military budgeting process allows for democratic participation and

[8] The definition of what is included in "military expenditure" varies. The most widely utilized data source for global military expenditure is from Stockholm International Peace Research Institute (SIPRI). SIRPRI's definition includes all current and capital expenditure on: the armed forces, including peacekeeping forces; defence ministries and other government agencies engaged in defence projects; paramilitary forces when judged to be trained, equipped and available for military operations; and military space activities – to include the costs of personnel (military and civil) including retirement pensions and social services for personnel and their families; operations and maintenance; procurement; military-related research and development; military construction; and military aid (in the military expenditures of the donor country):
http://www.sipri.org/research/armaments/milex/resultoutput/sources_methods/definitions

[9] The United Nations provides two sample forms for the submission of data, one simplified and one more detailed and disaggregated. States should fill out the more detailed form. The UN Office for Disarmament Affairs publishes information received a website: http://www.un.org/disarmament/convarms/Milex/html/MilexIndex.shtml

[10] Only nine countries (Cuba, Equatorial Guinea, Eritrea, Guyana, Myanmar, North Korea, Somalia, Turkmenistan, and Uzbekistan) have not released basic military expenditure data in recent years:
http://www.sipri.org/research/armaments/milex/researchissues/measuring_milex.

provides further protection against misappropriation of funds (corruption) or the misdirection of security forces for political or personal interests.

Recommendations:

1. Governments publish a detailed legislative proposal for the coming year's military budget with sufficient lead time to permit open debate and amendment before the budget is finalized.
2. Governments publish all contracts for procurement of military or other equipment over a reasonable threshold (threshold will vary depending on the government's level of military expenditure). In order to minimize corruption relating to military procurement, governments should maintain a national, publicly accessible database of all major procurement contracts.[11]
3. Military spending is subject to an annual independent audit, including all sources of revenue. The audit report should be published and locally accessible.
4. Submit information on weapons holdings and transfers to the United Nations Register on Conventional Arms.

Country Examples: The UK National Audit Office provides a model information portal on oversight of MOD budgeting, including clear and concise descriptions of the content of various audits and reports.[12] India also has a comprehensive military auditing system.[13] The UN created a register of conventional weapons holdings and trade in 1991, following the Gulf War. The UN "Transparency in Armaments" initiative invites states to provide data annually on the preceding year's military holdings, procurement through national production, and arms transfers in an effort to encourage restraint in the production or transfer of arms and to help identify excessive or destabilizing accumulations of weapons. Although participation has flagged somewhat in recent years, since its inception, 173 states have submitted reports to the UN Register on one or more occasions.[14]

III. Most Ambitious Steps

Goal: Governments disclose a top-line figure for intelligence spending, as well as information about component intelligence agency budget lines, and establish parliamentary and external oversight bodies to ensure the integrity of expenditures and operations.

Justification: The secretive nature of the work of intelligence services, their recourse to special powers, and their operation at the margins of the law have resulted in most governments shrouding this area of public expenditure in complete secrecy. In the past decade, as global concerns about terrorism have grown, intelligence services have been endowed with ever greater powers of collection and freedom of operation, and they now consume a larger share of public funds. These trends have generated renewed awareness about the need for effective

[11] See, for example, http://www.USAspending.gov and http://www.defense.gov/contracts/
[12] http://www.nao.org.uk/publications/1011/mod_performance_2009-10.aspx
[13] http://cgda.nic.in/index.html
[14] http://www.un.org/disarmament/convarms/Register/DOCS/2010-11-01_RegisterFactSheet.pdf

oversight structures—both to ensure that intelligence services conduct their work in compliance with the rule of law and international human rights standards and to protect against corruption concerning this highly secretive and unaccountable sector. Increased budget transparency and the establishment of independent oversight bodies are necessary to provide basic public accountability.

Recommendations:

1. Governments publish their overall budget for intelligence, with disaggregated budget lines for different intelligence component agencies or services and/or selected functional activities (e.g., collection, analysis, covert action).

2. Governments create some form of select oversight body and process (executive, legislative, and/or judicial) that monitors the detailed budget and operations of the intelligence agencies.

3. Governments establish an independent oversight body with the powers needed to review effectively the raw intelligence and assess, in some manner, the outputs in order to help ensure against misuse or politicization of the information.

Country Examples: In recent years, governments of the UK, Canada, and the Netherlands have published their overall intelligence spending levels, with no apparent or claimed negative security consequences.[15] The Dutch Government furthermore publishes the amount spent on "confidential expenditures" and also notes the percentage of the budget devoted to staff expenses, user allowance, and operational management and task funds.[16] In 2007, the US began reporting the aggregated national intelligence budget figure for the preceding fiscal year,[17] and in October 2010 the Secretary of Defense disclosed the size of the military intelligence program budget for the first time.[18] In February 2011, the US Office of the Director of National Intelligence announced that the US Government was requesting $55 billion in national intelligence budget for fiscal year 2012, marking the first time that the top-line figure has been released publicly before Congress has acted to appropriate the funds.[19] In South Africa, the National Assembly's Joint Standing Committee on Intelligence oversees the budgets and operations of all intelligence agencies. In the US, a Select Committee on Intelligence in each the House and the Senate set the budget levels and oversee policy behind closed doors.

[15] See Federation of American Scientists, Secrecy and Government Project, website at http://www.fas.org/irp/budget. Also "Annual Report 2008-2009, Intelligence and security Committee," chairman Rt. Hon. Dr. Kim Howells, MP, pp. 4-6

[16] General Intelligence and Security Service, Ministry of the Interior and Kingdom Relations [NL], Annual Report 2009, p. 61.

[17] As required by Public Law 110-53, since 2007 the US Director of National Intelligence discloses the aggregate amount of funds appropriated by Congress for and expended by the National Intelligence Program for the preceding fiscal year within 30 days after the end of the fiscal year. The NIP budget includes only the amount that is not devoted purely to military operations. For fiscal year 2010 that figure was $52.1 billion.

[18] Ken Dilanian, "Overall U.S. intelligence budget tops $80 billion," Los Angeles Times, October 28, 2010.

[19] Brian Clampitt , "U.S. Intelligence Budget Request Revealed," Harvard National Security Journal blog, Feb 23, 2011, http://harvardnsj.com/2011/02/intelligence-budget-request-revealed/

National Security[20]

No questions are more important to ensuring democratic government and fundamental human rights than those involving decisions about war, peace and protection of a country's national security. Inherent in this truism, however, is a fundamental tension. On the one hand, democracy and respect for fundamental human rights depend on public access to government information: access to information not only safeguards against abuse by governments, officials and private entities working with them, but also permits the public to play a role in determining the policies of the government. On the other hand, the conduct of diplomacy, military operations and intelligence activities all require some measure of secrecy in order to be effective.

Striking the right balance is made all the more challenging by the fact that courts in most countries demonstrate the greatest deference to the claims of government when national security is invoked. This deference is reinforced by provisions in the security laws of many countries that trigger exceptions to the right to information as well as to ordinary rules of evidence and rights of the accused upon a minimal showing or assertion of a national security risk. A government's over-invocation of national security concerns can seriously undermine the main institutional safeguards against government abuse: independence of the courts, the rule of law, legislative oversight, media freedom, and open government.

I. Initial Steps

Goal: All public bodies that handle national security information, including the armed forces, ministry of foreign affairs, intelligence and special services, are covered by access to information and proactive disclosure requirements, subject only to specific and limited exceptions approved by the legislature.

Justification: Security sector and other agencies that handle national security information should be covered by access to information laws or other disclosure obligations for at least four reasons:

1. Application of such laws reaffirms both to the entities and the public that security sector agencies, like all public bodies, are subject to the rule of law and democratic accountability.

[20] OSF thanks the following organizations for their assistance in developing these sample commitments: Africa Freedom of Information Centre (Africa), American Civil Liberties Union (US), Centre for Applied Legal Studies, Witwatersrand University (South Africa), Centre for National Security Studies (US, international), Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University (Argentina, Latin America), Commonwealth Human Rights Initiative (India, Commonwealth), Conectas - Human Rights (Brazil, global south), Egyptian Initiative for Personal Rights (Egypt), Fundar (Mexico), Geneva Centre for Democratic Control of the Armed Forces (Europe, international), Institute for Information Freedom Development (Russia), Institute for Defense Security and Peace Studies (Indonesia), Institute for Security Studies (Africa), National Security Archive (US, international), Open Democracy Advice Centre (South Africa, southern Africa), OpenTheGovernment.org (US), and Project on Government Oversight (US).

2. Application of disclosure obligations has led to exposure of wrongdoing, mismanagement and threats to public safety, health and the environment that might not otherwise have come to light.

3. Exceptions in access to information and related laws have proved effective in protecting information that truly does need to remain secret. We are not aware of any instances in which disclosure of information pursuant to an access to information law resulted in harm to national security that exceeded the public interest in knowing the information.

4. Intelligence and security agencies produce a great number of documents that are invaluable to researchers, scholars and the public that do not reveal anything about confidential government actions. For instance, the US Central Intelligence Agency (CIA) holds extensive documents concerning Saddam Hussein's history of human rights abuses. None of these documents reveal anything about US policies or CIA activities, but they do reveal a great deal of information of public interest about what Saddam Hussein did and what and when the US knew about these abuses.

Recommendations:

- States should pass or amend their laws, or the Head of State should issue a decree, to make clear that all public bodies that handle national security information are subject to disclosure requirements. Specific and limited categories of information that must be kept secret to protect the nation's security – such as identities of sources, and intelligence gathering techniques – may be exempted by statute.

- The existence of all public bodies, including intelligence entities, should be publicly disclosed, as well as contact numbers, budgets and general powers and authorities of such bodies.

- States should preserve police, military and intelligence archives, should open them to the public to the extent not inconsistent with protecting legitimate national security interests, and should criminalize the willful destruction or alteration of records unless expressly permitted by law.

- States should establish bodies to review the decisions of security sector agencies to withhold information. Such oversight bodies should be autonomous, adequately resourced, and equipped with the powers needed to fulfill their mandates.

- No information should remain classified indefinitely. The presumptive maximum period of secrecy on national security grounds should be established by law and should be subject to extension only in exceptional circumstances and by a decision-maker independent of the initial classifier.

Country examples: India's Right to Information Act 2005 applies to all branches of the armed forces, the Ministry of Defense, the Coast Guard, the Department of Atomic Energy, nuclear power plants, aeronautics and space research organizations (except the Aviation Research Centre), and state civilian and armed police organizations.[21] The Act allows intelligence and security services to be exempted from the law,[22] but Parliament can debate any exclusion and force the government to withdraw it. Moreover, all security and intelligence agencies, even those excluded from the purview of the RTI Act, are obliged to disclose information about allegations of corruption and human rights violations committed by their officials and employees.[23] In the US, no agency may be entirely exempted from the Freedom of Information Act (FOIA); only "operational files" of intelligence agencies – e.g., informants' identities, and secret methods of information gathering that would be ineffective if revealed -- may be exempted, and only by a statute duly passed by both Houses of Congress.[24] For instance, a bill to exempt the operational files of the Defense Intelligence Agency was defeated in 2000 because the bill, if passed, would have shielded the activities of foreign death squads, torturers and other human rights abusers.[25] More recently, President Obama ordered that no category of intelligence information may be kept forever secret, and the CIA is now disclosing its highest level President's briefs from the 1960s. The interagency appeals panel (ISCAP) has ruled in favor of disclosing CIA documents in more than 60% of cases, illustrating the value of an appeals panel that is independent, includes representatives of several agencies, and is adequately resourced. Knowing that files may not be kept secret forever has had a significant positive effect on promoting archival programs and good governance in general.

II. More Substantial Steps

Goal: States make public, and do not classify, information about human rights violations, corruption and other serious wrongdoing, including information needed by victims to obtain redress or by prosecutors to bring criminal charges.

Justification: States increasingly are adopting access to information, secrecy and related laws that expressly state that information about human rights violations, corruption or other serious crimes may not be withheld or classified, and must be provided on request. States have adopted mandatory transparency provisions for several reasons: disclosure of such information deters wrongdoing, facilitates accountability, promotes good governance, and helps victims obtain some satisfaction. Moreover, adherence to the principle of open justice is crucial to guard against excessive judicial deference to the executive and to ensure respect for human rights

[21] Right to Information (RTI) Act, sec. 2(h).

[22] Sec. 24 of India's RTI Act provides that the Central Government and any state governments may add any intelligence or security organization to a list of bodies exempted from the Act.

[23] RTI Act, Sec. 24(2) and (4) require that "information pertaining to allegations of corruption and human rights violations shall not be excluded."

[24] "Operational files" of several intelligence agencies--including the Central Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office and the National Security Agency--are exempted by statute from the FOIA pursuant to 5 U.S.C. § 552 (b)(3), which exempts materials "specifically exempted from disclosure by statute."

[25] *See* Archive Calls on CIA and Congress to Address Loophole Shielding CIA Records From the FOIA, National Security Archive Electronic Briefing Book No. 138, "Proliferation of the Problem," (Oct. 15, 2004), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB138/index.htm.

even during periods when vital national interests are under threat.[26] Only in exceptional circumstances may the high public interest in knowing about torture and other serious abuses be overridden, namely, when the state can establish that disclosure of information would pose an identifiable, likely and significant risk of serious harm to a legitimate and important national security interest.

Recommendations:

- States should pass laws that explicitly state that information about human rights violations, corruption or other serious wrongdoing may not be classified or otherwise withheld from the public. Best practice is to disclose such information proactively.
- States should commit to not invoke national security as a ground for denying Information that an individual needs either to establish that he/she was the victim of a human rights violation or is not guilty of a criminal offense.

Country examples: The laws of more than a dozen countries -- including Albania, Ecuador, Guatemala, India, Mexico, Peru, Romania, Russia and Uruguay -- expressly provide that information about human rights violations, violations of law in general, and/or corruption may *not,* under any circumstances, be classified or withheld, and some provide that such information must be disclosed proactively.[27]

III. More Ambitious Steps

Goal: Mechanisms exist to ensure that public servants, including members of intelligence services and special forces, are able to report evidence of serious wrong-doing to independent oversight bodies without fear of retaliation; public servants are able to report such evidence to the media and public without fear of criminal punishment; and the media and other members of the public are able to publish and disseminate such reports without fear of punishment.

Justification: Numerous regional and national bodies, from the Council of Europe to more than 20 national governments, are currently reviewing their laws and policies to increase protections for public sector personnel who disclose information that reveals serious wrongdoing. It is increasingly recognized that protections for insiders (sometimes called "whistleblowers") is a

[26] See e.g., *R (Binyam Mohamed) v. Secretary of State for Foreign and Commonwealth Affairs* (No 4) [2009] 1 WLR 2653 ["BM (No 4)"], 36; and [Court of Appeal] 131.

[27] Mexico's Federal Transparency and Access to Public Government Information Law 2002 includes a clause in Article 14 that explicitly overrides exceptions when the information is "related to the investigation of a severe violation of fundamental rights or crimes against humanity." Romania's RTI law provides that "information that favors or conceals the violation of the law by a public authority or institution" cannot be classified and should be disclosed in the public interest. Law no. 544/2001 of the 12th of October 2001 on Free Access to Information of Public Interest, Article 13. Article 7 of the Russian Federal Law on State Secrets states that "It is not allowable to classify information regarding violations of human rights and illegal wrongdoing by state bodies and their officials." Albania's Law on Classified Information states that "[c]lassification shall be prohibited when made with the intent of covering up (suppressing) violations of the law, or failures or the ineffectiveness of the state administration; depriving a person, organization or institution of the right of access [to the relevant information]; or preventing or delaying the disclosure of information whose protection is not justified by national security interests." Sec. 10 of Law No. 8457 of Feb 11, 1999 on Prohibition of Classification.

crucial element of any strategy to effectively combat gross misuse of resources and abuse of power, and to ensure that the public has access to information needed to participate meaningfully in policy making as well as to protect against threats to public safety, health and the environment. Moreover, experience shows that the most effective way to deter leaks of classified or otherwise secret information is through career incentives and disincentives and pursuit of policies that are recognized as legitimate, not through use of criminal law or penalties directed against public servants. Criminal prosecution of media and other information disseminators for reporting government information is inconsistent with democratic principles and freedom of the press. Genuinely sensitive information is best protected through the use of narrowly drawn statutes criminalizing disclosure of clearly defined and limited categories of information whose disclosure would likely cause identifiable and significant harm to national security that is not outweighed by the public interest in knowing such information.

Recommendations:

- Members of the public, including the media, should be able to publish information without fear of criminal prosecution or other official sanction or penalty, in order to safeguard the crucial role of the media and social watchdogs in promoting democratic governance.

- Public sector personnel, including members of the intelligence services and other security sector agencies, should be authorized, and indeed encouraged, to provide information to oversight bodies of serious wrongdoing, mismanagement, or threats to public safety, health or the environment, without fear of retaliation, so long as they reasonably believe the information to be accurate. Such reports should be properly investigated and appropriate remedial steps taken. Security procedures should be established to enable these disclosures to occur while keeping secret the identity of the whistle-blower as well as, where necessary, the reported information itself.

- Public sector personnel should not be criminally prosecuted for disclosing to the public information concerning serious wrongdoing, mismanagement, or threats to public safety, health or the environment if they have exhausted internal reporting procedures or if internal reporting would likely be fruitless or subject them to retaliation.

- Before public sector personnel are subject to sanctions of any sort beyond paid administrative leave for disclosing classified information to the public in violation of any oath, agreement or rule, they first must be afforded full due process rights by law and in practice, including a fair hearing before a body independent of the agency seeking to impose sanctions.

- No journalist should be compelled to reveal a confidential source or unpublished materials in an investigation concerning unauthorized disclosure of information to the press or public.

Country examples: The European Court of Human Rights ruled in 2008 that the dismissal by the Government of Moldova of an employee in the prosecutor's office for making disclosures to a newspaper concerning pressure from public officials to dismiss criminal proceedings against police officers constituted an unlawful interference with the employee's right to impart information. The unauthorized leak could be justified in light of the lack of an alternative, effective remedy; the public interest in and truthfulness of the information, which outweighed any harm caused by the disclosure; and the employee's good motive.[28] During the period 2007-2010, the Parliamentary Assembly of the Council of Europe undertook a study of whistleblower protection regimes in Europe and other parts of the world and adopted a set of principles to serve as a guide to its member States for instituting similar legislation.[29] These principles include robust protections for "protected disclosures," defined to include "all bona fide warnings against various types of unlawful acts, including all serious human rights violations which affect or threaten the life, health, liberty and any other legitimate interests of individuals as subjects of public administration or taxpayers." Governments throughout Europe, the Americas and other parts of the world have started to domesticate and implement many of these principles.

***

For more information, please contact:

Anthony Richter, ARichter@sorosny.org
or
Sandra Coliver, scoliver@justiceinitiative.org
400 West 59th St
New York, NY

Morton Halperin, mhalperin@osi-dc.org
1730 Pennsylvania Ave, NW
Washington DC

[28] Guja v. Moldova, Eur. Ct. of Human Rights (2008), App. No. 14277/04.
[29] These principles are contained in Resolution No. 1729 of the Parliamentary Assembly of the Council of Europe, available at: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/ERES1729.htm, last accessed on August 12, 2011.

OPEN SOCIETY FOUNDATIONS

OPEN GOVERNMENT PARTNERSHIP
SECURITY SECTOR
SAMPLE COMMITMENTS

September 2011