6/10/2013

Guidance for Implementing Section 5 of E.O. 13636
Privacy and Civil Liberties Protections

We uphold our fundamental principles and values not just because we choose to, but because we swear to. Not because they feel good, but because they help keep us safe. They keep us true to who we are . . .. So as Americans, we reject the false choice between our security and our ideals. We can and we must and we will protect both.

President Barack Obama

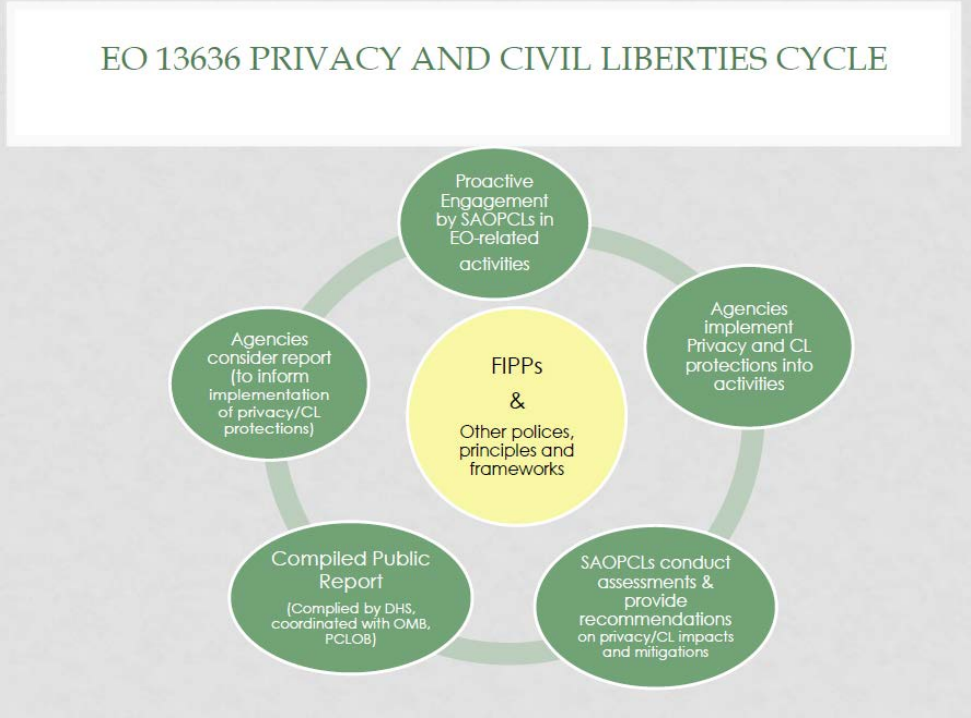
Background

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, (the E.O.) directs federal departments and agencies to establish, expand or prioritize a number of activities to improve cybersecurity for U.S. critical infrastructure. Many of these activities raise concerns regarding their potential impact on individual privacy and civil liberties. Section 5 of the E.O. requires department and agency Senior Agency Officials for Privacy and Civil Liberties (SAOPCLs) to incorporate privacy and civil liberties protections into such activities, and to conduct assessments of those activities, based upon Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks. E.O. 13636 §5 (a) and (b). It is important to note that the processes required by the E.O. are in addition to, not a replacement of, an agency's existing processes to ensure compliance with all applicable laws and other Executive Orders and policy directives.

SAOPCLs and other agency staff have requested that the National Security Staff (NSS) provide written guidance on implementing E.O. Section 5, and on the conduct of the required privacy and civil liberties assessments. This document is intended to assist SAOPCLs and their staff in developing agency-specific processes to implement Section 5, and to encourage consistency across the federal community, to the extent practicable, in assessment of privacy and civil liberties impacts and protection in E.O.-related agency activities. **The E.O., however, makes SAOPCLs responsible for developing privacy and civil liberties protections, and conducting assessments, appropriate to their individual agency's E.O. activities, authorities, and mission. These guidelines are intended to provide a springboard for SAOPCL efforts to implement Section 5 of the E.O., but they are not a substitute for, nor should they override, the professional judgment and analysis of individual SAOPCLs.**

PART I: The Privacy and Civil Liberties Protections Cycle

E.O. Section 5 establishes a privacy and civil liberties protection and oversight cycle.



All of the steps of the cycle are centered around implementing protections based upon, and evaluating activities against, Fair Information Practice Principles and other applicable polices, principles and frameworks to protect individual privacy and civil liberties. For more about the FIPPs, see Part II below.

Step One: Proactive Engagement and Identifying E.O. Activities.
Agencies are required to coordinate their E.O implementation activities with SAOPCLs. E.O. 13636 §5 (a). SAOPCLs should engage proactively with agency operators engaged in cybersecurity activities and cybersecurity policy to determine: (1) What activities the agency is engaged in to implement the E.O. (agency E.O. activities); and (2) Whether/how privacy and civil liberties protections are being considered and incorporated in those implementation activities. SAOPCLs are expected to identify their own agency's activities by engaging directly with agency personnel. The list of sample E.O.-related activities provided in Appendix A may assist SAOPCLs in identifying E.O. implementation activities in which their agency may be participating.

Step Two: Implementing Privacy and Civil Liberties Protections
In addition to identifying agency E.O. implementation activities, SAOPCLs also must coordinate with their agency operators to ensure adequate privacy and civil liberties protections are incorporated into those activities, applying FIPPs and other applicable policies, principles and frameworks. E.O. 13636 §5 (a)

Step Three: Agency Privacy and Civil Liberties Assessments and Recommendations

SAOPCLs are required to assess the privacy and civil liberties risks of their agency E.O. activities as implemented, and may make recommendations for additional ways to mitigate or minimize such risks. In other words, each agency's assessments should describe, at a minimum, the agency E.O. activities conducted, the privacy and civil liberties risks and impacts associated with each E.O. activity, and any privacy and civil liberties protections undertaken to mitigate or minimize those risks and impacts. SAOPCLs have discretion to provide assessments of activities that are in development, or to defer providing an assessment until an activity is implemented. In the case of deferral, however, the SAOPCL should identify the activity and describe the reasons for deferring the assessment for the Compiled Public Report. SAOPCLs may also include their recommendations (if any) for ways to further reduce the privacy and civil liberties risks or impacts of each activity.

The E.O. requires SAOPCLs to conduct privacy and civil liberties assessments independent of assessments conducted by other agencies and interagency input. Agencies are NOT expected to assess activities conducted outside their agency and should refrain from opining on activities in which their agency is not directly engaged. E.O. 13636 §5 (b).

Step Four: Compiled Public Report

SAOPCLs must provide their written assessments to the Department of Homeland Security (DHS). DHS Privacy Office and Office for Civil Rights and Civil Liberties will compile those assessments and incorporate them into the public report required under E.O. 13636 §5 (b) (the Compiled Public Report). DHS will coordinate interagency and OMB review of the Compiled Public Report contents. DHS must also ensure consultation with the Privacy and Civil Liberties Oversight Board. E.O. 13636 §5 (c). The first Compiled Public Report must be released no later than February 14, 2014. The report must be reviewed and updated annually.

Step Five: Agency Review and Consideration of the Compiled Public Report

Agencies are required to review and consider the entire Compiled Public Report as they continue to implement and assess agency E.O. activities. E.O. 13636 §5 (b). SAOPCLs should take steps to ensure that appropriate agency personnel review and consider the final report. Agencies should continue to identify and assess agency E.O. activities. Future assessments of agency E.O. activities should address how report recommendations, if any, have been incorporated.

PART II: Applying the FIPPs and Other Applicable Policies, Principles, and Frameworks

What are the FIPPs?

Fair Information Practice Principles (FIPPs) are the widely-accepted framework of defining principles used to assess and mitigate privacy and civil liberties impacts of information systems, processes, or programs. The FIPPs are eight interdependent principles--Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. These principles form a framework that can be applied to any type of information collection, use or disclosure; the exact implementation of each principle, however, will vary based upon context.

- **Transparency:** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- I**ndividual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

See National Strategy for Trusted Identities in Cyberspace, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf (April 2011).

The FIPPs are not a new invention of this E.O. To the contrary, they are time-tested and universally recognized principles. They were first articulated by the U.S. Department of Health, Education and Welfare report "Records, Computers and the Rights of Citizens" in 1973. They form the basis of the Privacy Act of 1974, and can be found in dozens of federal privacy and information protection statutes, dating back to 1971. They also form the basis for many international data privacy frameworks, including the OECD Privacy Guidelines and the APEC Privacy Principles. More recently, the FIPPs were adopted as the defining framework for privacy in the cybersecurity context in the White House's National Strategy for Trusted Identities in Cyberspace (April 2011). They also form the basis for the Consumer Privacy Bill of Rights, promulgated in the Administration's Blueprint for Consumer Privacy in a Networked World (February 2012).

Why FIPPs?

The FIPPs are the foundational principles of government information privacy. Because the FIPPs are principles, not rules, they can be applied regardless of the existing legal or policy framework. They apply across government missions--in cybersecurity, national security, law enforcement, benefits administration, etc. They provide an objective set of principles to evaluate privacy and civil liberties impacts of programs, but permit agencies to apply them in the context of their differing authorities and missions. They do not conflict with or contravene existing intelligence or law enforcement authorities; rather, they suggest ways to mitigate privacy impacts as practical for the information collection/mission context. Some have argued that FIPPs hamper effective information sharing. This is a myth. Appropriately applied, the FIPPs enable effective information sharing by identifying and safeguarding key values for any information sharing program—such as data accuracy, relevance, timeliness, and security

How Should FIPPs Be Applied in E.O. Activities and Assessments?

The FIPPs are a framework for identifying and evaluating privacy risks, impacts and mitigations; not a check list of "absolutes." SAOPCLs should consider how each principle may be applied to each agency E.O. activity. Assessments should describe:

- The agency E.O. activity being assessed
- How each FIPP is implemented in that activity
- FIPPs that are not fully implemented for that activity and why
- Compensating controls (for example, other policies or methods) that may mitigate the privacy or civil liberties risks and impacts

For example, an Agency may provide "transparency" for a cybersecurity program through varied means—such as Privacy Impact Assessments, briefings or reports to Congress or other stakeholders, and websites or other public media. In conducting an assessment of the program as an agency E.O. activity, SAOPCLs should describe and refer to all means of transparency the agency employs. In contrast, that same program may not include a mechanism for "individual participation." The assessment should describe why individual participation is not included, and what other mechanisms are implemented to ensure information accuracy and to provide redress for individuals suffering unintended harms.

Appendix B provides sample questions to assist SAOPCLs in evaluating agency E.O. activities against FIPPs.

What Other Policies, Principles and Frameworks Should Apply?

Civil Liberties Considerations in Cybersecurity

First and Fourth Amendments: The First Amendment prohibits Congress from passing any law that prohibits the free exercise of religion or abridges freedom of speech, freedom of the press, the right of the people to assemble peaceably, or the right to petition the government for redress of grievances. As applied, this also prohibits the Government from discriminating on the basis of viewpoint, or of taking any other steps that would tend to "chill" the right to free speech or free association. The Fourth Amendment provides protection from unreasonable search and seizure—including "search" or interception of electronic communications. These Constitutional rights may be implicated by programs that monitor lawful activities or communications. Agencies should consider whether agency E.O. activities involve the monitoring or interception of communications, or compiling of information regarding lawful activities, as well as the legal authorities and procedures undertaken to safeguard individual rights in carrying out such activities.

Fifth Amendment: The Fifth Amendment protects individuals against the exercise of government authority without due process of law. Agencies should consider whether agency E.O. activities could involve government actions that may interfere with individual rights, including property rights and rights to due process.

Appendix B provides sample questions to assist SAOPCLs in evaluating agency E.O. activities that may implicate civil liberties considerations.

Other Policies/Frameworks:
Agencies may have additional policies, principles or frameworks that apply to cybersecurity activities and information sharing. For example, the Intelligence Community has guidelines for the handling of information relating to U.S. persons, and to protect sources and methods. Law enforcement agencies have special considerations for information that is related to an investigation or other law enforcement activities. Some agencies may have policies related to the particular sensitivity of the information that they collect or distribute, such as financial or health information.

These other policies, principles or frameworks may or may not be directly related to privacy and civil liberties protections. If the policy, principle or framework has an impact on how PII and other cybersecurity information is handled and protected, however, its application to agency E.O. activities should be described in activity assessments. Accordingly, when such a policy, principle or framework applies to an agency E.O. activity, it should be described in the assessment for that activity, and the impact on privacy and civil liberties protections and risks should be assessed. For example, a directive for intelligence activities may prevent an agency from providing public transparency or individual participation in its cybersecurity activity. The assessment of that activity should address that impact, as well as any compensating controls—such as accuracy, correction and oversight safeguards--that are in place to protect individual privacy and civil liberties.

PART III Coordination and Oversight Review of Compiled Report

The E.O. requires each agency to provide its assessments to DHS. The DHS Privacy Office and Office for Civil Rights and Civil Liberties are responsible for compiling those assessments into a single public report. Appendix C provides a simplified format for agencies to report assessments to DHS. This format, however, is intended only as a guide.

Assessments Working Group

To ensure proper interagency coordination, DHS has established an interagency Assessments Working Group, consisting of representatives of the privacy and civil liberties officials of agencies involved in implementing the E.O. The purpose of this group is to provide a forum for assisting SAOPCLs in meeting their responsibilities under the E.O. It is important to note, however, that individual agency SAOPCLs remain responsible for the content and conduct of assessments of their own agency E.O. activities. In addition, although the Assessments Working Group may assist in coordinating interagency review and input into the Compiled Public Report, the E.O. makes the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties ultimately responsible for compiling the report and ensuring its timely release.

Interagency Coordination

Agencies should provide DHS with final assessment reports for inclusion in the CompiledPpublic Report. Accordingly, agency SAOPCLs are responsible for ensuring their assessments are appropriately reviewed and cleared through their internal agency processes prior to providing them to DHS. The DHS Privacy Office and Office for Civil Rights and Civil Liberties, in consultation with the Assessments Working Group, may set deadlines for submission of such reports—including deferring inclusion of material received after the deadline.

The draft Compiled Public Report will undergo interagency review through the Cybersecurity Interagency Policy Council (Cyber IPC). Comments will be reviewed and adjudicated by the DHS Privacy Office and Office for Civil Rights and Civil Liberties. DHS also will coordinate review by the OMB and the PCLOB.

Classified Information

Agency E.O. activities may involve classified operations or information. Such activities should be assessed in the same manner as unclassified activities. The results of such assessments should be provided to DHS through secure channels and included in an appropriately classified annex to the Compiled Public Report.

Appendix A: Sample Agency Activities Related E.O. 13636

Note: This Appendix provides examples of agency activities related to E.O. 13636 and its implementation. This list is intended to be illustrative only; SAOPCLs should identify agency E.O. activities that involve privacy and civil liberties risks.

Sample Agency Activities (specific agencies leading/coordinating activity)
Develop instructions to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity, and a process that rapidly disseminates information in compliance with the instructions. (DHS, DNI, DOJ)
Establish procedures to expand Enhanced Cybersecurity Services (ECS) to all critical infrastructure sectors. (DHS, DOD)
Provide reports on analysis of incentives for participating in the voluntary cybersecurity program, including recommendations on the feasibility, security benefits, and relative merits of such incentives and incorporating security standards into acquisition planning and contract administration. (DHS, Treasury, Commerce, GSA, DOD)
Identify critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security. (DHS, Sector Specific Agencies)
Develop a Framework of core cybersecurity practices to reduce cyber risks to critical infrastructure that incorporates existing voluntary consensus standards and industry best practices. (NIST)
Establish a voluntary program to promote the adoption of the cybersecurity practices defined in the Framework, incorporating incentives where appropriate (DHS, Sector Specific Agencies)
Executive branch agencies responsible for regulating the security of critical infrastructure will report on authorities needed to address cybersecurity risks to critical infrastructure.
Executive branch agencies responsible for regulating the security of critical infrastructure will propose actions to mitigate cyber risk, if needed.

Appendix B: Sample Assessment Questions and Considerations

Note: This Appendix provides example questions and potential issues for privacy and civil liberties assessments of E.O. activities as a reference guide. This list is intended to be illustrative only; SAOPCLs should develop assessment questions and methods to identify privacy and civil liberties risks, impacts and mitigations specific to their agency E.O. activities.

Sample FIPPs-Focused Questions/Issues**:**

Transparency:

- How is the general public informed about the activity?
- If the activity involves PII, how do the individuals identified by that PII receive notice describing the collection, use, sharing and maintenance of that information?

I**ndividual Participation:**

- Does the activity include opportunity for individuals to consent to the collection/use/sharing/maintenance of PII in the activity?
- Are individuals provided opportunity to access and correct PII collected/used/shared/maintained in the activity? If so, how?
- What mechanisms are available to provide redress for misuse of PII or adverse outcomes based upon the use of PII in the activity?

Purpose Specification:

- For what specific purposes is PII collected/used/shared/maintained in the activity?
- How are individuals or the general public made aware of those purposes?

Data Minimization:

- What PII is relevant and necessary to the activity?
- How does the agency ensure the PII collected is relevant and necessary to the activity?
- How does the agency ensure PII is expunged after it is no longer relevant and necessary?

Use Limitation:

- How does the agency ensure agency use of the PII is limited to the purposes specified and compatible purposes?

Data Quality and Integrity:

- What mechanisms are used to ensure PII is accurate and complete for the purpose for which it is used?
- What controls are in place to ensure PII is up to date?
- What methods are used to identify and eliminate obsolete PII?

Security:

- How is PII secured in transit and as stored in the activity?
- What safeguards are in place to protect the PII against unauthorized disclosure?
- What procedures are in place to identify and address potential security vulnerabilities in systems holding and to address potential breach of, PII related to the activity?

Accountability and Auditing:

- What protections are in place to ensure electronic communications are not inadvertently captured and stored?
- What safeguards are in place to ensure that purpose specification and use limitations are maintained?
- What methods are used to evaluate the efficacy of transparency and individual participation mechanisms?
- What additional agency oversight mechanisms apply to the activity?
- Is there a procedure for regular review of the activity for compliance with privacy and civil liberties safeguards? Are there sufficient audit logs/records to enable such oversight?

<u>Sample Civil Liberties-Focused Questions/Issues:</u>

- What specific statutory, order or directive gives the agency the authority to conduct the activity?
- Does the activity involve collection or use of PII or communications content that could create a chilling effect on protected behavior such as free speech and/or freedom of association?
- Could the activity result in denial of a benefit, service or right to an individual?
- Does the activity involve making assumptions or drawing inferences about individuals based upon demographics or the content of their communications?
- Are PII or communications linked to an individual in such a way as to create or imply a stigma or other adverse impact upon the individual?
- Could the activity result in disclosure of information about an individual beyond the individual's intent or expectation? Disclosure of information relating to third parties?
- Does the activity involve targeting individuals for additional or increased monitoring of future activities or communications based on protected status?
- Does the activity involve targeting individuals for additional or increased monitoring or scrutiny based upon opinions or beliefs expressed, or other elements of communications content?
- What safeguards are in place to mitigate privacy and civil liberties risks or impacts for these activities?

Appendix C: Sample Assessment Report Format

Note: This Appendix provides a simplified report format as a guide. Members of the Assessments Working Group, as led by DHS, may revise or replace this format to meet its needs.

E.O. Implementation Activity:

[Describe the activity being assessed, and the agency's role in that activity.]

Privacy and Civil Liberties Risks/Impacts:

[Describe how the activity may impact individual privacy and civil liberties. This section should describe the use, collection, maintenance or disclosure of personally identifiable information as part of the activity]

FIPPs Analysis:

Transparency:
[Describe methods of implementing transparency for the activity; any barriers to providing transparency; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Individual Participation:
[Describe methods of implementing individual participation for the activity; any barriers to providing such participation; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Purpose Specification:
[Describe methods of implementing purpose specification for the activity; any barriers to purpose specification; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Data Minimization:
[Describe methods of data minimization for the activity; any barriers to implementing data minimization; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Use Limitation:
[Describe methods of use limitation for the activity; any barriers to implementing use limitations; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Data Quality and Integrity:
[Describe methods ensuring data quality and integrity for the activity; any barriers to ensuring data quality and integrity; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Security:
[Describe methods securing PII in the activity; any barriers to securing PII; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Accountability and Auditing:
[Describe methods of providing accountability for the activity; any barriers to implementing accountability and auditing; the risks and impact of those barriers on individual privacy and civil liberties; any compensating controls or measures taken to mitigation those risks and impacts.]

Other Privacy and Civil Liberties Considerations:

[Describe other policies or privacy or civil liberties risks and impacts that are implicated by the activity. Provide analysis of how those policies are implemented and how such risks are mitigated.]

Recommendations:

[Make recommendations, if any, to mitigate privacy and civil liberties risks and impacts identified in the assessments]