

Fusion Centers Get New Privacy Orders Via DHS Grants

by [Harley Geiger](#) [1]

December 15, 2009

Last Tuesday, the Department of Homeland Security (DHS) [announced](#) [2] [2]the release of guidance for awarding grants for 2010. That Friday, the DHS Privacy Office publicly highlighted a provision of the [guidance](#) [3] [3]for the Federal Emergency Management Agency's (FEMA) grant program that relates to fusion centers. The grant program requires fusion centers to certify compliance with the privacy and civil liberties [guidelines](#) [4] [5]of the Information Sharing Environment (ISE).

Under the DHS grant guidelines, fusion centers must certify that their privacy and civil liberties protections are as comprehensive as the ISE Guidelines within six months of the grant award. To make this certification, the fusion centers must have had their privacy policies reviewed and on file with the ISE Privacy Guidelines Committee. Otherwise, the grant funds for fusion centers may be used only to develop the fusion centers' privacy protections.

Fusion centers and other domestic intelligence agencies have been the subject of several high-profile civil liberties controversies within the past year. (CDT blogged about these events [here](#) [6], [here](#) [7]and [here](#) [8].) Tying fusion centers' grant funds to the ISE Privacy Guidelines is a very positive step forward in ensuring fusion centers protect civil liberties, although it should be one of several important steps that include strengthening the ISE Guidelines themselves.

Tip of the Fuse

Fusion centers gather crime and terrorism-related information from a variety of sources, including law enforcement officers, private sector entities and anonymous tipsters. They analyze or "fuse" this data in an attempt to identify patterns of terrorist or criminal operations and to provide reports to a range of organizations, such as other government agencies at the state, local and federal level. There are approximately 70 fusion centers around the country.

Federal strategy calls for sharing fusion center data nationwide through the Information Sharing Environment (ISE) program. The ISE is essentially a means of connecting the data-gathering efforts of law enforcement agencies on the local, state and federal level. For example, the ISE would streamline the ability of local police departments to share information gathered on potential terrorism suspects with the FBI or National Counterterrorism Center (NCTC), with fusion centers envisioned as an intermediary between local/state and federal agencies.

A Good Start, but Only a Start

The ISE was established by law under the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. IRTPA also required the ISE to protect Americans' privacy and civil liberties in carrying out its mission of sharing terrorism information among law enforcement agencies. To fulfill this statutory requirement, the Program Manager for the ISE developed a set of privacy and civil liberties guidelines. The ISE Guidelines are supposed to apply to all the agencies that will constitute the ISE, including fusion centers.

The ISE Guidelines are comprehensive in scope, generally following the widely accepted [Fair Information Practices](#) [9]. However, the Guidelines also lack depth in some key areas. In many places, the ISE Guidelines require only that participant agencies have a policy in place, with scant specifics on how that policy should be carried out. For example, the ISE Guidelines' requirement for Data Security is "*Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.*"

The generalized nature of the ISE Guidelines makes it difficult to assess compliance among participant agencies in the absence of blatant violations, and there are no clear penalties for noncompliance. This difficulty is exacerbated by a convoluted chain of command. Currently

information sharing oversight responsibilities seem to be neither comprehensive nor unambiguous. State bodies with varying structures and varying degrees of effectiveness most directly [supervise](#) [10]. [10]many frontline ISE participants, such as local police departments and fusion centers. Reports from both [DHS](#) [11]. [11]and [GAO](#) [12] cite particular difficulty in overseeing state and local fusion centers, as they are not subject to many of the same statutes and oversight bodies as federal agencies. The ISE Guidelines urge participant agencies to consult the [Privacy and Civil Liberties Oversight Board](#) [13] for ongoing guidance in protecting civil liberties in participants' use of the ISE - but the Board currently has no members and has been inactive for nearly two years.

The newly-released DHS grant requirements help to a limited extent. Requiring that a fusion center's privacy protections are as comprehensive as the ISE Guidelines is important, but the ISE Guidelines' ambiguousness runs the risk that some fusion centers will establish similarly vague and toothless policies. Moreover, the grant requirements do not solve the problem of oversight and enforcement once the award is made - there is no grant requirement, for example, that the fusion center must actually follow its own policy or lose the funding. Although the federal grant process has some audit mechanisms, it is unclear whether those mechanisms will be limited to checking whether the fusion center has certified its privacy policy and submitted the policy for review.

The entire information sharing cycle should be subject to comprehensive monitoring with clear penalties for noncompliance. One or more independent entities must have the express authority and responsibility to audit every ISE participant, as well as to limit a participant's connections to the ISE for chronic noncompliance. Oversight bodies must monitor participants' compliance with their own policies and ensure those policies conform to or exceed the Privacy Guidelines in practice, not just on paper.

The DHS grant requirements are a welcome move towards incentivizing fusion centers to protect privacy, hopefully the first of more substantial moves to come.

- [privacy](#)
- [security](#)
- [National security](#)
- [grants](#)
- [data](#)
- [DHS](#)
- [CDT](#)

Copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants>

Links:

[1] <https://cdt.org/personnel/harley-geiger>

[2] http://www.dhs.gov/ynews/releases/pr_1260283102665.shtm

[3] http://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_kit.pdf

[4] <http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf>

[5] <http://www.ise.gov/public/docs/privacy/PrivacyGuidelines20061204.pdf>

[6] <http://www.cdt.org/blogs/harley-geiger/fusion-paranoia-and-bad-policy>

[7] <http://www.cdt.org/blogs/harley-geiger/us-intelligence-reports-continue-confuse-political-dissent-terrorism>

[8] <http://www.cdt.org/blogs/harley-geiger/thwarting-civil-liberties-problem-domestic-intelligence>

[9] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[10] <http://homeland.house.gov/SiteDocuments/20090401102139-35729.pdf>

[11] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf



[12] <http://www.hsaj.org/pages/supplement/issue2/pdfs/supplement.2.3.pdf>

[13] <http://www.cdt.org/blogs/heather-west/cdt-urges-white-house-move-pclob>