# DOES NCTC HAVE THE MINIMAL DATA SECURITY TO GUARD ITS NEW NOT-TERRORIST-TERRORIST DATABASE?

As I noted here and here, yesterday the Director of National Intelligence and DOJ rolled out new Guidelines allowing the National Counterterrrorism Center to acquire non-terrorist datasets from federal agencies—including US person data—so they can do pattern analysis on those datasets and pass off the resulting data to other agencies.

When intelligence officials wanted to explain to Charlie Savage how this would work, they pointed to a State Department dataset—visa applications—as one dataset NCTC might now access directly.

> A person from Yemen applies for a visa and lists an American as a point of contact. There is no sign that either person is a terrorist. Two years later, another person from Yemen applies for a visa and lists the same American, and this second person is a suspected terrorist.
>
> Under the existing system, they said, to discover that the first visa applicant now had a known tie to a suspected terrorist, an analyst would have to ask the State Department to check its database to see if the American's name had come up on anyone else's visa application — a step that could be overlooked or cause a delay. Under the new rules, a computer could instantly alert analysts of the connection.

The State Department is, of course, still

reportedly recovering from the fact that because of DOD's lax network security, 250,000 diplomatic cables got liberated for the world to see.

Not surprisingly, then, the new Guidelines appear determined to reassure original dataset owners that their data won't be compromised by sharing it with NCTC (which can then share it with other elements of the Intelligence Community and even foreign allies). You can tell they're serious about this, because it's one of the places they occasionally use "shall" (in other sensitive areas, they use the squishier "will").

> For access to or acquisition of specific datasets, the DNI, or the DNI's designee, shall collaborate with the data provider to identify any legal constraints, operational considerations, privacy or civil rights or civil liberties concerns and protections, or other issues, and to develop appropriate Terms and Conditions that will govern NCTC's access to or acquisition of datasets under these guidelines.
>
> [snip]
>
> In addition to the [general requirements laid out for sharing this data], at the time when NCTC acquires a new dataset or a new portion of a dataset, the Director of NCTC shall determine, in writing, whether enhanced safeguards, procedures, and oversight mechanisms are needed.

Though this bold approach almost immediately breaks down, as the Guidelines not only revert to "will," but—worse—dig out the passive voice when describing the data transfer.

> Measures will be put into place to ensure that the dataset is received and stored in a manner to prevent unauthorized access and use prior to the completion of replication.

And when the Guidelines get into specifics, they use that passive "will" again.

> Access to these datasets will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation, and changes, and queries executed, in according with audit and monitoring standards applicable to the Intelligence Community.

**Who** will ("shall") implement these data security measures? What if he or she fails to do so adequately?

It's a really, really important question because—as this year's intelligence authorizations make clear, the Intelligence Community does not yet have insider threat detection—the kind of security that would permit these audits—and they're not going to get it until 18 months from now. Hell, they're not even going to start getting it until 6 months from now!

> (a) Initial Operating Capability.—Not later than October 1, 2012, the Director of National Intelligence shall establish an initial operating capability for an effective automated insider threat detection program for the information resources in each element of the intelligence community in order to detect unauthorized access to, or use or transmission of, classified intelligence.
>
> (b) Full Operating Capability.—Not later than October 1, 2013, the Director of National Intelligence shall ensure the program described in subsection (a) has reached full operating capability.

Which is why I find this passage from the Guidelines so amusing (admittedly, at least here they use "shall" again).

> In designing its computer systems, NCTC shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, these Guidelines.

That is, in the Guidelines authorizing this data sharing, the government is ordering NCTC to put into place—in the future—the network security to adequately guard it.

And remember, NCTC can share the information that it gets from other entities with other members of the Intelligence Community, including DOD and its notoriously sieve-like network security. Not to worry, though! These guidelines have the same prospective language ordering IC community elements to design computer systems to make real auditing possible.

> In designing its computer systems, the IC element shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, this Appendix [guiding information sharing with IC elements].

In other words, as of yesterday, NCTC can get all the databases in the federal government which they claim might contain significant terrorism information. But even as they got that authority, they only spoke prospectively about implementing the basic network security they need to guard all this data.

Yesterday, the government created (at least in theory) the mother of all databases, including information on perfectly innocent American citizens. And yet even as it did so, it all-but

admitted the computer systems to adequately protect that database are not yet in place. Indeed, on Tuesday, the government's own experts admitted that our networks are still totally compromised.

And yet, when someone leaks all this data for public release (or when China and Iran use it to advance their own spying agendas) the government will act surprised, again, as they do every time their gaping security holes get compromised.