A WHOLE LOT OF INSPECTOR GENERAL SCRUTINY ON INTELLIGENCE COMMUNITY NETWORKS

Between this report, released today, on DOD Inspector General's ongoing work and the Intelligence Community's Inspector General Semiannual report, released in mid-January, the Intelligence Community is doing a whole bunch of audits and inspections of its own network security, some of them mandated by Congress. And there are at least hints that all is not well in the networks that enable the Intelligence Community to share profusely.

The most interesting description of a report from ICIG's Semiannual review, for example, suggests that, given the IC's recent move to share everything on an Amazon-run cloud, the bad security habits of some elements of the IC are exposing other elements within the IC.

> ### *AUD-2015-006: Transition to the Intelligence Community Cloud Audit*
>
> The DNI, along with Intelligence Community leadership, determined that establishing a common IT architecture across the IC could advance intelligence integration, information sharing, and enhance security while creating efficiencies. This led to the Intelligence Community Information Technology Enterprise, an IC-wide initiative coordinated through the Office of the Intelligence Community Chief Information Officer. IC ITE's sharing capability is enabled by a

> cloudbased architecture known as the IC Cloud — a secure resource delivering IT and information services and capabilities to the entire community. The cloud will allow personnel to share data, systems, and applications across the IC. The IC elements' effective transition to the IC ITE cloud environment is key to achieving the initiative's overarching goals and as such, systems working together in a cloud environment creates potential security concerns.
>
> In particular, information system security risks or vulnerabilities to one IC element operating within IC ITE may put all IC elements at risk. <u>Information from a joint IG survey of 10 IC elements suggested that the elements may have the differing interpretations of policies and requirements, or are not fully aware of their responsibilities for transitioning to the IC Cloud</u>. As a result of these preliminary observations, IC IG initiated an audit that will: 1. Assess how the IC elements are planning to transition to the IC ITE Cloud environment; 2. Determine IC elements' progress in implementing cloud transition plans; and, 3. Compare how IC elements are applying the risk management framework to obtain authorizations to operate on the IC Cloud. We plan to issue a report by the end of the first quarter of FY 2017. [my emphasis]

The IC is banking quite a bit on being able to share safely within the cloud. I would imagine that fosters a culture of turf war and recriminations for any vulnerabilities. It certainly seems that this report arises out of problems — or at least the identification of potential problems — arising from the move to the cloud. Note that this report won't be completed until the end of this calendar year.

Then there’s this report, which was mandated in a classified annex of the Intelligence Authorization passed in December and, from the looks of things, started immediately.

> ### *Audit of Controls Over Securing the National Security Agency Network and Infrastructure (Project No. D2016-DOOORC-0072.000)*
>
> We plan to begin the subject audit in January 2016. Our objective is to determine whether initiatives implemented by the National Security Agency are effective to improve security over its systems, data, and personnel activities. Specifically, we will determine whether National Security Agency processes and technical controls are effective to limit privileged access to National Security Agency systems and data and to monitor privileged user actions for unauthorized or inappropriate activity. The classified annex to accompany H.R. 2596, the Intelligence Authorization Act for Fiscal Year 2016, contained a Department of Defense Inspector General classified reporting requirement. This audit is the first in a series. We will consider suggestions from management on additional or revised objectives.

It seems to be an assessment — the first in a series — of whether limits on privileged access to NSA systems are working. This may well be a test of whether the changes implemented after the Snowden leak (such as requiring two parties to be present when performing functions in raw data, such as required on dragnet intake) have mitigated what were some obviously huge risks.

I’m mostly curious about the timing of this report. You would have thought the implementation of such controls would come automatically with some kind of audit, but they’re just now, 2.5 years later, getting around to that.

Here are some other reports from the ICIG report, the latter three of which indicate a real focus on information sharing.

> ### *AUD-2015-007: FY 2015 Consolidated Federal Information Security Modernization Act of 2014 Capstone Reports for Intelligence Community Elements’ Inspectors General*
>
> This project will focus on FY 2015 FISMA report submissions from the OIGs for the IC elements operating or exercising control of national security systems. We will summarize 11 IC elements’ information security program strengths and weaknesses; identify the cause of the weaknesses in these programs, if noted by the respective OIGs; and provide a brief summary of the recommendations made for IC information security programs. To perform this evaluation, we will apply the Department of Homeland Security FY 2015 IG FISMA metrics for ten information security program areas.
>
> 1. Continuous Monitoring Management 2. Security Configuration Management 3. Identity and Access Management 4. Incident Response and Reporting 5. Risk Management 6. Security Training 7. Plan of Action and Milestones 8. Remote Access Management 9. Contingency Planning 10. Contractor Systems We will

issue our report by the end of the first quarter of FY 2016

INS-2015-004: Inspection: Office of the Intelligence Community Chief Information Officer

The IC CIO is accountable for overall formulation, development, and management of the Intelligence Community Information Technology Enterprise. The scope of our review was limited and informed by a concurrent IC IG Audit survey of IC ITE, as well as an ongoing evaluation of IC ITE progress by the ODNI Systems and Resources Analyses office. Additional details of this report are in the classified annex.

INS-2015-005: Joint Evaluation of Field Based Information Sharing Entities

Along with our OIG partners at the Departments of Justice and Homeland Security, we are evaluating federally supported entities engaged in field-based domestic counterterrorism, homeland security, and information sharing activities in conjunction with state, tribal, and local law enforcement agencies. This review is in response to a request from Senate committees on Intelligence, Judiciary, Homeland Security and Governmental Affairs. We will issue our report during FY 2016.

INS-2015-006: Inspection: ODNI Office of the Program

Manager–Information Sharing Environment

We last inspected the ODNI PM-ISE office in 2013 and are conducting a follow-up review with a focus on resource management.