by Rachel V. Rose and John Okray

An Interview with Robert Litt—General Counsel of the Office of the Director of National Security

Share with us your background and how you evolved into your role as general counsel of the Office of the Director of National Intelligence (ODNI).

I began my legal career as a federal prosecutor. After a number of years in private practice doing criminal and civil litigation, I returned to the Department of Justice in 1994 first as a deputy assistant attorney general in the Criminal Division and then as principal associate deputy attorney general. In those jobs I had my first exposure to intelligence and national security law, reviewing [Foreign Intelligence Surveillance Act] FISA applications, participating in reviews of covert action programs, and dealing with a variety of national security policy issues.

In 1999 I returned to private practice. The awful events of Sept. 11, 2001, had an emotional impact on me, as they did on so many others, reinforcing my desire to return to government. Over the next years I did some speaking and writing on matters relating to national security and civil liberties. In addition, I represented members of the intelligence community in several matters. After President Barack Obama was elected, Adm. Dennis Blair, who had been selected to be Director of National Intelligence (DNI), asked if I would be his general counsel, and I was nominated by the president and confirmed by the U.S. Senate.

The ODNI is an agency that some may not be familiar with. Would you please describe what the office does?

The ODNI was established by the Intelligence Reform and Terrorism Prevention Act of 2004 as a result of recommendations of the 9/11 Commission. By statute, the Director of National Intelligence has three functions:

- First, he is the head of the intelligence community. In addition to the ODNI, the intelligence community includes the Central Intelligence Agency; the National Security Agency; the National Geospatial-Intelligence Agency; the Defense Intelligence Agency; the National Reconnaissance Office; and intelligence elements of the Federal Bureau of Investigation, the Drug Enforcement Administration, the military services, the Coast Guard, and the departments of Energy, Treasury, State, and Homeland Security.
- Second, the DNI is the principal intelligence adviser to the president, the National Security Council, and the Homeland Security Council.
- Third, the DNI is responsible for overseeing and directing the implementation of the national intelligence budget.

Thus, the ODNI's responsibilities range from coordinating the preparation of the president's daily intelligence briefing to ensuring that adequate resources are allocated across the intelligence community to enable the collection and analysis of intelligence critical to national security priorities to drafting legislative proposals on intelligence-related matters.

The current DNI, James R. Clapper, has focused on using his authorities to further the integration of the intelligence community across the various agencies that make up the intelligence community and across the various disciplines (collection and analysis) and types of intelligence (such as human intelligence, signals intelligence, or open source).

How do you coordinate legal matters with the other 16 executive agencies in the U.S. intelligence community?

I am not the general counsel for the intelligence community. Each intelligence community element has its own lawyers, and my office has no authority to bind them. On the other hand, there are times when legal issues would benefit from coordination across elements or when lawyers for two or more intelligence community elements disagree. In those cases, we can act as an honest broker and bring together lawyers to try to reach a resolution that satisfies everyone. In addition, we have meetings of all of the general counsels approximately once a quarter to identify and discuss matters of common interest, and we have an annual conference for all of the lawyers of the intelligence community.

Rachel V. Rose, JD, MBA, is the chair of the Corporate and Associations Counsel Division. She is the principal at Rachel V. Rose — Attorney at Law PLLC (Houston) and co-author of The ABCs of ACOs *and* What are International HIPAA Considerations? *She can be reached at* rvrose@rvrose.com. *John Okray, JD, MBA, LCM, is the chair of the Health Law Section. He is a co-author of* The ABCs of ACOS.

There is often a tension between privacy and security. How do you balance these competing interests legally and ethically?

I don't think that we should think in terms of a "balance" between privacy and security. I believe that the correct approach is to seek to protect both security and privacy in a time when we are facing wide-ranging and dispersed threats, when the growth of technology has presented both opportunities and challenges for collection, and when globalization and digital communications have made it far harder simply to isolate the communications of your adversaries. I believe that our legal and policy doctrines need to take account of changing technology, not only to recalibrate our expectations of privacy but also to find ways to use technology as a means to protect privacy while protecting security.

Cybersecurity is an issue on the forefront of every business and government agency's agenda. What do you perceive as the biggest threats related to security attacks?

In his unclassified Annual Threat Assessment testimony this year, Director Clapper noted that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The unclassified networks that support U.S. government, military, business, and personal users are likely to remain vulnerable to both espionage and disruption. More likely than a cyber-Armageddon scenario that debilitates the entire U.S. infrastructure is a continuing series of low- to moderate-level cyber intrusions and attacks from a variety of sources, which will impose cumulative costs on U.S. economic competitiveness and national security. These threats will come from a range of actors, including nations with highly sophisticated cyber programs (such as Russia or China); nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea); profit-motivated criminals; and ideologically motivated hackers or extremists. The incentive to conduct cyber espionage and cyberattacks is great because of the relative ease of these operations, the potential gain to their perpetrators, and the difficulties of attribution.

In March, the House Intelligence Committee passed the Protecting Cyber Networks Act (PCNA), a near-identical image of the cybersecurity data-sharing bill known as Cyber Information Sharing Act (CISA), which passed in the Senate. What is your perspective on these two pieces of legislation?

There are actually *four* cyber bills in play: the Senate's Cybersecurity Information Sharing Act; the Protecting Cyber Networks Act, offered by the House Permanent Select Committee on Intelligence (HPSCI); the House Homeland Security Committee's National Cybersecurity Protection Advancement Act; and the administration's own cyber bill, which was submitted to the U.S. House and Senate back in January. Obviously, there is a lot of interest in doing something in the realm of cybersecurity and cyberinformation sharing. In my view, which bill makes it across the finish line (if any) will come down to two issues: (1) liability protections, a significant feature in each of the bills but noticeably broader in both House bills and the Senate bill, and (2) authorization for the private sector to use defensive cybermeasures, which is contained in both the HPSCI and Senate bills but not in the administration bill. In the administration's view, liability protections should encourage good cybersecurity practices and not immunize a company for failing to act on information it receives about the security of its own network. As for defensive measures, improper use of defensive measures could actually undermine cybersecurity. We are committed to improving cyberinformation sharing, however, and look forward to working with congressional counterparts on an appropriate solution.

How would these initiatives impact your office?

I don't believe that either piece of legislation would have a substantial impact on my office.

The intelligence community has consistently been rated in the top 10 best places to work in the federal government (No. 4 in 2014 among large agencies and in the top quartile). Why do you believe intelligence community employees have such a high level of job satisfaction? How would you compare ODNI versus your prior public and private sector positions?

I am fond of telling young lawyers considering a career in public service that except for twice a month, on pay day, the worst days in government service are better than the best days in private practice. I find it immensely rewarding to leave the office each day knowing that I have spent the day working on behalf of the American people. In addition, the problems are endlessly interesting and challenging, and the people I work with—both the wonderful lawyers in my office and the outstanding personnel in the intelligence community—are smart, thoughtful, and enjoyable colleagues. I think that people throughout the intelligence community feel the same way about defending the nation, and that's why the job satisfaction is so high.

What are your goals as general counsel of the ODNI? How will you measure success in your role?

I suppose I have two overall goals. One relates to the operation of the ODNI. When I started as general counsel, ODNI was less than 5 years old. Many of its authorities, processes and structures were still being fleshed out, and I hope that by the time I leave as general counsel, we will have succeeded in putting the agency on a firm footing going forward. Second, Director Clapper has made his focus integrating the intelligence community—trying to continue the process of moving away from the stovepiped, agency-centric structure that existed pre-9/11 to an integrated community that works together across disciplines and agencies. I would like to move the intelligence legal community in the same direction—not eliminating individual agency legal offices or subsuming them but inculcating a perspective that looks at legal problems from a communitywide perspective and seeks solutions that work for the entire community in the interest of the nation. ⊙