NATIONAL INTELLIGENCE UNIVERSITY

Ann Caracristi Institute For Intelligence Research

What this is:

This report is the product of academic research. As the IC's university, NIU is uniquely positioned to use academic approaches to research—and report on—subjects of interest to the community.

What this is not:

This is not finished intelligence. The opinions expressed in this report are solely the author's and not those of National Intelligence University, or any other US Government agency.

RESEARCH SHORT

CATALYST Designed to spark positive conversations on the future of the IC

September 4, 2024

IMAGES FROM SHUTTERSTOCK

Unveiling Public Safety: The Power of Declassification

Deb Pfaff, Ph.D., and Trisha Ripley

Substantial public safety benefits derive from declassifying information related to private sector security. From declassification of the US military's Global Positioning System to actionable warnings of terrorist activities and Russia's plans to invade Ukraine, intelligence sharing has fostered private sector technology development and risk management strategies that better protect US national security and public safety. Providing the US public with knowledge that can safeguard the populace has undeniable intrinsic value, but transparency and the free flow of critical information also foster trust, enhance understanding, and promote beneficial public-private partnerships.

Secrecy and Transparency: A Tug of War

The relationship between government secrecy and public transparency is, and always has been, a matter of tug of war. There is an inherent push and pull of preserving national security while upholding democratic ideals and principles. This tension is profoundly necessary, as certain information must remain protected from public exposure, avoiding the risks of aiding malicious actors or revealing intelligence sources and methods. But the Intelligence Community (IC) has historically leaned heavily in favor of classifying almost anything that crosses its doorstep, even if this information is already well known in the public sphere. The origin of COVID-19 is one example; the IC released a declassified report on COVID-19's origins long after the public was already aware that the virus originated from one of two sources in China.[1]

> **"Whenever the people are well informed, they can be trusted with their own government."**
>
> — Thomas Jefferson

The practice of overclassification isn't just costly,* although the financial, time, and personnel burdens of declassification are substantial.[2, 3] Declassifying intelligence—or not classifying some information in the first place—can serve a broader purpose by offering a public safety benefit. Declassification instills a greater trust in intelligence authorities, facilitates more informed decisionmaking, supports scientific research and innovation, and promotes international collaboration. Private sector security is a leading area that would be better able to help protect public safety through regularized access to shared intelligence.

Strengthening Private Sector Security To Enhance Public Safety

Declassification of information can have benefits for the private sector—from the growth of joint research efforts and multisector collaboration, to stimulating economic growth and investment by unlocking restricted information—that ultimately strengthen national security. Declassification of real-time, actionable intelligence helps private sector partners more effectively address *shared* security challenges—such as the growing array of cyber threats, supply chain vulnerabilities, and critical infrastructure risks that plague both the public and private sectors.

Release of previously classified information through vetted dissemination channels such as the Domestic Security Alliance Council (DSAC) can foster innovation and cross-sector collaboration, as declassified data can contain valuable insights for the US Government's private sector partners into past research, development, and technologies.[4] The value of such IC-private sector collaboration is particularly evident in joint research efforts that have led to technology transfer and the US Government's adoption of commercial technologies for use in space.[5] One prominent example of the latter is SpaceX, which has conducted cargo resupply missions, sent astronauts to the International Space Station, and

* Overclassification is estimated to cost $18 billion per year, with a 400-million-page backlog of classified documents in queue for declassification review. (*Sources:* Senator Ron Wyden and Senator Jerry Moran, "Time To Fix a Broken Declassification System," *Just Security*, September 8, 2020, https://www.justsecurity.org/72326/time-to-fix-a-broken-declassification-system/; and Patrick G. Eddington et al., "Bad Idea: Overclassification," *Defense360* (blog), Center for Strategic and International Studies, December 6, 2019, https://defense360.csis.org/bad-idea-overclassification/.)

developed the Artemis program for lunar exploration, in addition to ongoing collaboration with the IC on a range of classified efforts to advance US reconnaissance and surveillance capabilities.[6, 7, 8, 9]

Access to declassified intelligence or threat assessments can help businesses better understand potential risks and vulnerabilities, allowing them to develop more effective risk management strategies that support US national security. Declassification can also enhance security by promoting greater transparency and accountability that bolster public trust in US Government activities.[10, 11] This improved understanding between government and private sector entities can lead to more effective cooperation in addressing shared security challenges in a time of dwindling and unpredictable US Government budget cycles.

In recent years, several declassification efforts by the IC have provided timely warning to private sector partners that, in turn, took actions in the interest of public safety and security:

- The rapid declassification of sensitive intelligence with US critical infrastructure and cyber security partners—and the public writ large—in the runup to the Russian invasion of Ukraine in February 2022 helped fortify private sector security and mitigate cyber risks. US Government leaders noted that the declassification efforts in the form of cyber advisories to partners served to "prebunk" Russian disinformation efforts by preemptively refuting falsehoods with evidence-based factors before they could gain traction.[12, 13] The IC's release of detailed information before the invasion, while still protecting sources and methods, allowed allied partners to prepare evacuation routes out of Ukraine for noncombatants, develop alternative supply chains, and collaborate on broader cyber defenses, as noted during a panel discussion among private sector leaders.[14, 15] Policymakers have noted that such "prebunking" tactics could serve as a future model for addressing the threats posed by other adversaries, including China.[16]

- As a reaction to ongoing terrorism threats and in compliance with the Intelligence Reform and Terrorism Prevention Act of 2004, IC elements have collaborated to declassify intelligence or share terrorism-related tearlines—portions of an intelligence report approved for disclosure—that provide actionable warnings, while still safeguarding sensitive sources and methods.[17] This effort was most clearly seen in the takedown of the Islamic State of Iraq and ash-Sham and other terrorist online propaganda by Western security services, technology sector partners, and social media companies, including halting the livestreaming of a 2019 synagogue attack in Germany.[18, 19, 20] Grassroots and partner-led efforts including Tech Against Terrorism[21] and the Global Internet Forum to Counter Terrorism[22, 23] have helped to institutionalize exchanges of counterterrorism information in addition to public-private cooperative organizations and forums such as InfraGard, DSAC, Corporate Security Symposiums, and the Overseas Security Alliance Council.[24, 25]

- The strategic decision by the Department of Defense to declassify the Global Positioning System (GPS) for civilian use beginning in 1983,[26] and fully in 2000,[27] has promoted technological innovation and enabled capabilities that enhance public safety, including in-car navigation and location-based services.[28, 29, 30] The integration of GPS technology into smartphones revolutionized navigation with ride-sharing applications, such as Uber and Lyft, and

delivery services, such as FedEx and UPS,[31] which ensured food and medication deliveries during COVID-19 lockdowns. GPS technology aids disaster management and emergency response by providing accurate location data for affected areas, coordinating rescue efforts, and ensuring timely delivery of aid.[32] It further allows scientists to track animal migrations, monitor environmental changes, and conduct geological surveys.[33]

Such new and innovative public-private partnerships are helping to solve national security challenges, such as violent extremism, and fostering improved collaboration among national laboratories and private sector partners. As noted by a startup leader at an In-Q-Tel-sponsored briefing, "the US Government needs to get outside its comfort zone in sharing information and exercise this muscle."[34]

Current US information-sharing approaches are overwhelmingly focused on US Homeland protection and security, reactive in nature to information requests, and handled by DHS and the FBI. The IC can assist and protect private sector partners when US national security interests are at stake by creating information flows that are more proactive in nature, encompass domestic and international security trends, and are seen as a responsibility of most IC agencies, including the CIA and the Department of State's Bureau of Intelligence and Research (State/INR). Even steps short of declassification—such as broadening dissemination of lower classified intelligence to those with appropriate clearances—would open valuable information-sharing pathways. The preference by some IC agencies to publish finished intelligence exclusively on Top Secret systems has meant that Secret-cleared partners are unable to access resources potentially critical to their key judgments.[35]

Both the 2019 and 2023 *National Intelligence Strategy* publications and DNI testimony in recent years have noted how nonstate entities—from privately owned critical infrastructure to subnational entities managing our electoral infrastructure—are increasingly a major part of the national security attack surface.[36, 37, 38] As recommended by State/INR senior leaders, the IC must cultivate a culture of responsible risk acceptance that encourages engagement with nonstate entities and promotes information sharing to support the mission, including writing for release. State/INR additionally notes the need to downgrade and declassify intelligence assessments to support diplomatic engagements and initiatives, or "intelligence diplomacy."[39]

A RAND Corporation commentary took the IC's information-sharing responsibility one step further when suggesting that Intelligence Community Directive 191, "Duty To Warn"—itself a declassified document[40]—should be revised. The commentary called on the IC to include in its duty to warn not just threats against individual lives, but also nonviolent threats against the private sector, such as cyber attacks, disinformation campaigns, and intellectual property theft. Such a change would recognize that the "threat surface is disproportionately outside the government" and keep everyone involved in US national security that much safer.[41]

How Can the IC Better Undertake Information Sharing and Transparency...

Another tug of war is at work here. Secrecy infuses every aspect of the intelligence profession and, therefore, IC culture. The community needs to rethink the impact that secrecy has on both the

profession and culture to accomplish real change, which calls for concrete actions and honest discussions. Even with our leaders exemplifying this mindset, as DNI Avril Haines and CIA Director William Burns did in a 2024 *Time* magazine article in which they acknowledged the value of intelligence sharing,[42] pressure needs to come from agitators—people not afraid of upsetting the status quo—within the ranks. These agitators need to push for change from where they are in their organization, to begin to crack the culture from the inside out.

MOVING FORWARD

Until transparency persistently produces results that secrecy cannot, the IC will largely view transparency as a one-off parenthetical, rather than a repeatable process.

- The IC needs to rethink its classification standards—first looking at how information can be shared in ways that protect sources and methods but also maximize transparency and trust with the American public. Creating a classification category for information releasable to the IC's private sector partners would be a good start. Consider the above-mentioned declassification of sensitive information before Russia's invasion of Ukraine, which strengthened private sector security and ultimately its support for Ukraine. Institutionalizing a straightforward process of declassification to meet specific public-private partnership goals would normalize the release of intelligence and could be useful in speeding the US response to a public safety crisis.
- As noted in *The 9/11 Commission Report,* "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge."[43] And, while replacing the traditional intelligence "need-to-know" presumption with that of "need-to-share," the IC could expand the 9/11 Commission's recommendation beyond intragovernmental sharing to include the IC's private sector security partners.
- The IC also needs to address overclassification issues deriving from intelligence officers classifying output "just to be on the safe side." Every one of us has unnecessarily classified an email asking a colleague to join us for lunch. This costs us both in resources and in mindset, and is a lazy practice—one that stops us from viewing unclassified output as anything other than a risk to be avoided. Until transparency persistently produces results that secrecy cannot, the IC will largely view transparency as a one-off parenthetical, rather than a repeatable process.

… While Mitigating Inherent Risks?

As the IC rethinks its classification standards, the community must be cautious about declassification efforts that could expose sensitive intelligence sources and methods. Without proper precautions, the IC risks deterring foreign liaison services, human sources, or would-be sources from passing secrets to the United States.[44] As noted by former US intelligence officials in a 2024 *Foreign Affairs* article, adversaries "can sometimes work backward to discover the source of that information… feed disinformation into it, or… arrest or harm the source."[45] One solution is to reveal key analytical judgments without disclosing the raw reporting.

- As seen in the faulty intelligence underpinning Iraq weapons of mass destruction analysis, the release of intelligence that turns out to be incorrect can severely damage the

IC's credibility and reputation.[46] The IC should look to release high-confidence key judgments and include critical caveats within the information that is released.[47]

In addition to the risks to sources and methods, relying on nongovernmental entities to responsibly handle intelligence from the IC could prove challenging. Adversaries could exploit sensitive information by exposing vulnerabilities and, once specific vulnerabilities or sensitive areas are publicly known, they can become targets for cyberattacks, terrorism, or other malicious activities. Publicly released intelligence is also subject to misinterpretation or being taken out of context, leading to misinformation and unnecessary concern. The complexity of intelligence data might not be easily understood by the public, leading to confusion and misinformed decisions. Finally, revealing vulnerabilities in private sector security could damage the reputation of businesses, leading to economic losses.

Still, as Thomas Jefferson observed more than 225 years ago, "Whenever the people are well informed, they can be trusted with their own government." The IC is currently drowning in a tsunami of digitally created classified government documents. As noted by the Information Security Oversight Office in 2021:

> History remains our best early warning system. It is highly likely that we will experience something like the pandemic again—or something even worse. We must absorb the lessons we have learned so painfully… and apply them to such future crises. This is especially true in applying them to update our classification and declassification systems and spending the necessary funds to expand and harden our secure communications capabilities.[48]

Selectively lifting the veil of secrecy could better inform our partners in protecting national security and public safety, fostering public trust in our government's honesty and openness. To do so, the IC needs to articulate and emulate a culture that promotes responsible risk acceptance.

Deb Pfaff, Ph.D., is an Associate Professor of Research with the Ann Caracristi Institute at National Intelligence University and co-director of NIU's Center for Truth, Trust, and Transparency. She has 22 years of government service, 19 with the IC. Before her time with NIU, Dr. Pfaff served in the analyst career field at DIA. She holds a doctorate in justice, law, and criminology from American University and a master of science in forensic science from The George Washington University.

Trisha Ripley is a Senior Partnerships Officer within ODNI, where she advances US national security interests on issues ranging from foreign malign influence to emerging technologies. Ms. Ripley has led change and built coalitions across the US Government for more than 20 years, including more than a decade as a strategic analyst and policy planner at the National Counterterrorism Center, and joint assignments at the FBI and Department of State. She holds a master of arts in international affairs from The George Washington University and a bachelor of arts in government and French from the College of William and Mary.

If you have comments, questions, or suggestions for a *Research Short* topic or article, please contact the NIU Office of Research and Engagement at **NIPress@niu.odni.gov**.

Endnotes

1 Office of the Director of National Intelligence, "Unclassified Summary of Assessment on COVID-19s Origins," Intelligence Community Assessment, August 27, 2021, https://www.dni.gov/files/ODNI/documents/assessments/Unclassified-Summary-of-Assessment-on-COVID-19-Origins.pdf.

2 Senator Ron Wyden and Senator Jerry Moran, "Time To Fix a Broken Declassification System," *Just Security,* September 8, 2020, https://www.justsecurity.org/72326/time-to-fix-a-broken-declassification-system/.

3 Patrick G. Eddington et al., "Bad Idea: Overclassification," *Defense360* (blog), Center for Strategic and International Studies, December 6, 2019, https://defense360.csis.org/bad-idea-overclassification/.

4 Arvin S. Quist, "Declassifying Classified Information," chap. 11 in *Principles for Classification of Information,* vol. 2, *Security Classification of Information* (Oak Ridge, TN: Oak Ridge National Laboratory, April 1993), https://sgp.fas.org/library/quist2/index.html.

5 Justin Doubleday, "NRO, NGA Expanding Commercial Industry Partnerships with New Awards in the Works," *Federal News Network,* August 25, 2022, https://federalnewsnetwork.com/intelligence-community/2022/08/nro-nga-expanding-commercial-industry-partnerships-with-new-awards-in-the-works/.

6 "NROL-186," National Reconnaissance Office, accessed August 22, 2024, www.nro.gov/Launches/launch-nrol-186/.

7 Sandra Erwin, "SpaceX Launches NRO's First Batch of Next-Generation Spy Satellites," *SpaceNews,* May 22, 2024, https://spacenews.com/spacex-launches-nros-first-batch-of-next-generation-spy-satellites/.

8 Katherine Tangalakis-Lippert, "SpaceX To Build Spy Satellites for US Intelligence, Report Says," *Business Insider,* March 16, 2024, https://www.businessinsider.com/spacex-contract-network-spy-satellites-us-intelligence-report-2024-3.

9 Stephen Slick and Joshua Busby, "2019 Public Attitudes on US Intelligence," Chicago Council on Global Affairs, September 4, 2020, https://globalaffairs.org/research/public-opinion-survey/2019-public-attitudes-us-intelligence.

10 Stephan G. Grimmelikjuijsen et al., "The Effect of Transparency on Trust in Government: A Cross National Comparative Experiment," *Public Administration Review* 73, no. 4 (July/August 2003): 575-86, https://onlinelibrary.wiley.com/doi/abs/10.1111/puar.12047.

11 Joshua Busby and Stephen Slick, "Glasnost for US Intelligence: Will Transparency Lead to Increased Public Trust?," Chicago Council on Global Affairs, May 24, 2018, https://globalaffairs.org/research/public-opinion-survey/glasnost-us-intelligence-will-transparency-lead-increased-public.

12 "Cybersecurity in Perspective: More than a Technology Challenge," The Aspen Institute: Aspen Security Summit (conference), June 12, 2023, https://www.aspeninstitute.org/events/cybersecurity-in-perspective/.

13 Christian Vasquez, "Ukraine Information Sharing a Model for Countering China, Top Cyber Official Says," *CyberScoop,* June 12, 2023, https://cyberscoop.com/information-sharing-china-threat/.

14 US House of Representatives, "Mobilizing our Cyber Defenses: Maturing Public-Private Partnerships to Secure US Critical Infrastructure," House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, 117th Congress, April 6, 2022, https://www.congress.gov/event/117th-congress/house-event/114611.

15 "Lessons Learned in Ukraine" (panel on private sector perspective), 5th Annual AIRIP Global Intelligence Forum, Association of International Risk Intelligence Professionals, September 14-15, 2022.

16 Vasquez, "Ukraine Information Sharing a Model for Countering China."

17 The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report,* August 21, 2004, https://govinfo.library.unt.edu/911/report/911Report.pdf.

18 Christopher Brennan, "US, Europe Hit ISIS Propaganda Channel in Coordinated Takedown," *New York Daily News,* April 27, 2018, https://www.nydailynews.com/2018/04/27/us-europe-hit-isis-propaganda-channel-in-coordinated-takedown/.

19 US House of Representatives, House Homeland Security Committee, DHS's Progress in Securing Election Systems and Other Critical Infrastructure, 115th Cong., 2d sess., July 11, 2018, https://www.congress.gov/event/115th-congress/house-event/108513/text.

20 Maura Conway et al., "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict & Terrorism* 42, No. 1-2 (2019); 141-60, https://www.tandfonline.com/doi/full/10.1080/1057610X.2018.1513984.

21 "Disrupting Terrorists Online," Tech Against Terrorism, accessed April 30, 2024, https://techagainstterrorism.org/home.

22 "Governance," Global Internet Forum to Counter Terrorism (GIFCT), accessed April 30, 2024, https://gifct.org/governance/.

23 "Content Incident Protocol," Global Internet Forum to Counter Terrorism (GIFCT), accessed April 30, 2024, https://gifct.org/content-incident-protocol/.

24 "DSAC Resources," Domestic Security Alliance Council (DSAC), accessed April 30, 2024, https://www.dsac.gov/about/dsac-resources.
25 "About Us," Overseas Security Alliance Council (OSAC), accessed April 30, 2024, https://www.osac.gov/About/AboutUs.
26 *Global Positioning System: A Comprehensive Assessment of Potential Options and Related Costs Is Needed* (Washington, DC: Government Accountability Office, 2013), https://www.gao.gov/products/gao-13-729.
27 The White House, Office of the Press Secretary, "President Clinton: Improving the Civilian Global Positioning System (GPS)," press release, May 1, 2000, https://clintonwhitehouse4.archives.gov/WH/New/html/20000501_2.html.
28 "GPS Overview," The Global Positioning System, accessed July 30, 2024, https://gps.gov/systems/gps.
29 Juquai McDuffie, "Why the Military Released GPS to the Public," *Popular Mechanics,* June 19, 2017, https://www.popularmechanics.com/technology/gadgets/a26980/why-the-military-released-gps-to-the-public/.
30 *GPS: Application and Accuracy* (Washington, DC: Government Accountability Office, 2010).
31 AJ Agrawal, "How GPS Revolutionized Technology Today," *HuffPost,* May 12, 2017 (updated), https://www.huffpost.com/entry/how-gps-revolutionized-te_b_9917232.
32 "Civilian Applications of GPS–Public Safety and Disaster Relief ," website of the Los Angeles Air Force Base, accessed July 30, 2024, https://www.losangeles.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/734557/civilian-applications-of-gps-public-safety-and-disaster-relief/.
33 Kristen A. Schmitt, "New Tracking Technology Reveals Hidden Animal Migration Routes," *Smithsonian Magazine,* January 8, 2019, https://www.smithsonianmag.com/science-nature/technology-gps-collar-reveals-hidden-animal-migration-routes-180971185/.
34 "In-Q-Tel Insights Presents: Commercial Technology in Conflict—The Role of US Startups in Ukraine, Israel, and the Future of Warfare," In-Q-Tel (conference), 14 March 2024.
35 William R. Evanina, "Security Clearances in the Age of Social Media," Office of the Director of National Intelligence, May 13, 2016, https://www.dni.gov/index.php/newsroom/news-articles/news-articles-2016/1590-security-clearances-in-the-age-of-social-media.
36 Director of National Intelligence, *National Intelligence Strategy of the United States of America 2019,* accessed July 30, 2024, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.
37 Director of National Intelligence, *National Intelligence Strategy 2023,* accessed July 30, 2024, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf.
38 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community,* February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
39 Brett M. Holmgren, "The Future of Intelligence Support to Diplomacy," Remarks of the Assistant Secretary of State, Bureau of Intelligence and Research, at the University of Texas, September 12, 2022, https://www.state.gov/the-future-of-intelligence-support-to-diplomacy/.
40 Office of the Director of National Intelligence, "Duty to Warn," Intelligence Community Directive 191, July 21, 2015, https://www.dni.gov/files/documents/ICD/ICD-191.pdf.
41 Cortney Weinbaum, "The Intelligence Community Doesn't Warn About All Attacks Against the US Homeland. Why Not?" *RAND Corporation Commentary,* October 21, 2022, https://www.rand.org/pubs/commentary/2022/10/the-intelligence-community-doesnt-warn-about-all-attacks.html.
42 Massimo Calibressi, "Inside the White House Program To Share America's Secrets," *Time,* March 11, 2024, https://time.com/6835724/americas-intelligence-secrets/.
43 The National Commission on Terrorist Attacks Upon the United States, "Summary of Recommendations," *The 9/11 Commission Report* (Washington, DC: US Government Accountability Office, 2004), https://www.gao.gov/products/b-303692.
44 David V. Gioe and Michael J. Morell, "Spy and Tell: The Promise and Peril of Disclosing Intelligence for Strategic Advantage," *Foreign Affairs,* May-June 2024, https://www.foreignaffairs.com/united-states/spy-and-tell-gioe-morell.
45 Gioe and Morell, "Spy and Tell."
46 The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, "Unclassified Version of the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," March 31, 2005, https://www.govinfo.gov/app/details/GPO-WMD.
47 The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, "Unclassified Version of the Report."
48 Information Security Oversight Office, "2021 Annual Report to the President, July 26, 2022," https://www.archives.gov/files/isoo/reports/isoo-2021-annual-report-to-the-president-final.pdf.