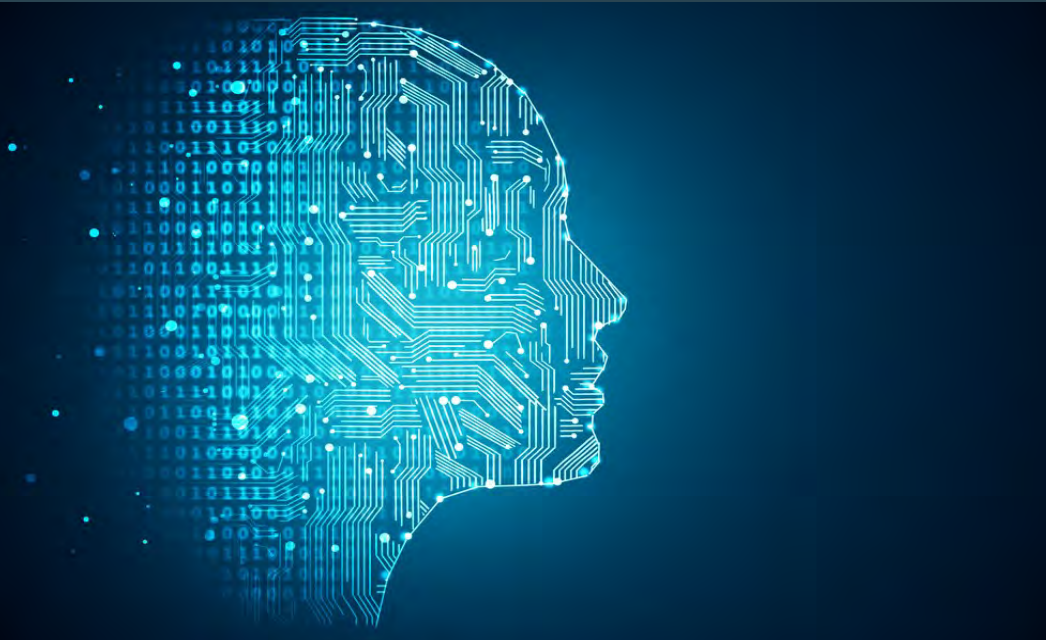




FEDERAL PARTNER NEWSLETTER

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER



National Artificial Intelligence Research Institutes

Maria Fernanda Pembleton, Communications Specialist, Computer and Information Science and Engineering, U.S. National Science Foundation

Over the past several decades, artificial intelligence (AI) has been the basis for critical advances in a wide range of fields, including nearly every field of scientific discovery as well as education, agriculture, transportation, climate science, and many more. Increased computing power, the availability of large datasets, and algorithmic advances in AI have begun to revitalize entire industries and create new sectors of the economy.

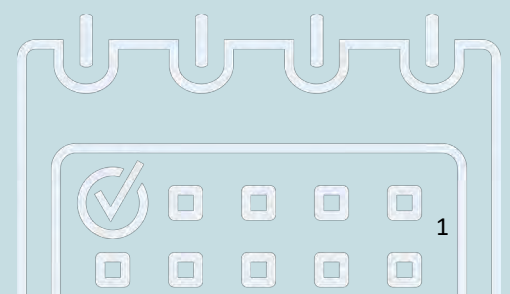
The National Artificial Intelligence Research and Development Strategic Plan, created by an interagency working group under the auspices of the White House Office of Science and Technology Policy, calls for a unified effort between government, academia and the private sector to prioritize AI research and development as well as education and training opportunities to prepare the American workforce for the new era of AI.

In addition, the National Artificial Intelligence Initiative, which became law in January 1, 2021, and the 2021 National Security Commission on Artificial

UPCOMING EVENTS

- ◆ July 21, 2021 : CDSE Webinar – Overview of Personnel Vetting Methodology
- ◆ July 29 : CDSE Webinar - Organizational Culture and countering insider Threat: Best Practices from Marine Corps Insider Threat Hub
- ◆ August 3 – 5 : CDSE Webinar – Department of Defense Virtual Security Conference
- ◆ August 25 : Quarterly Federal Partners CI Roundtable
- ◆ August 26, 2021 : CDSE Webinar – Overview of the National Background Investigation Services
- ◆ September 2, 2021 : Insider Threat Virtual Conference

*See events in SAGE for links





“ We are now reaping the harvest of 40 years of investment by federal agencies, including the NSF and the Defense Advanced Research Projects Agency, in long-term, fundamental AI research, and we must ensure that seeds are planted and nurtured for the decades ahead. ”

Intelligence report, establish a framework for an AI research infrastructure that democratizes access to the resources that fuel AI development across the nation, and a national network of AI research institutes.

In 2019, the U.S. National Science Foundation (NSF), in collaboration with other federal agencies, launched the National Artificial Intelligence Research Institutes program to fund a series of AI research centers across the nation. Each institute is funded at up to \$20 million over 5 years and includes multiple academic, industry, and government partners. The AI Institutes support foundational and translational research in AI technology and its application to vital sectors of the economy, as well as education and workforce development for the next generation of AI talent. In 2020, awards were made to five institutes managed by NSF and two institutes funded and managed by the U.S. Department of Agriculture National Institute of Food and Agriculture. The institutes comprise more than 130 organizations across 22 states. An additional cohort of institutes will be announced in the summer 2021, and planning is underway for another solicitation. “The Institutes will develop the new scientists and the new ideas that will drive research, translation, and commercialization forward. But as big as the program is – the current total

budget across the next 5 years is over \$300 million – it is small compared to the benefits it will provide, and still only a down payment on what is needed to maintain our position in the global AI race.”

“We are now reaping the harvest of 40 years of investment by federal agencies, including the NSF and the Defense Advanced Research Projects Agency, in long-term, fundamental AI research, and we must ensure that seeds are planted and nurtured for the decades ahead,” said Henry Kautz, Director of the NSF Division of Information and Intelligent Systems.

“The National AI Research Institutes are a vital first step toward ensuring U.S. leadership in AI – and by extension, ensuring our country’s economic future,” continued Kautz. “

Weighing the Benefits and Risks of AI in a Government Context

*Steven Babitch,
Head of Artificial Intelligence,
GSA’s Technology Transformation Services*

From the conversations I’m having with many in the federal community, many senior leaders are still in the early stages of understanding what AI is, what it’s not, and whether or not to invest in such technologies, given the wide variety of concerns surrounding the use of AI.. They understandably question whether the benefits outweigh the risks.

There are real benefits to the use of AI technologies, whether in creating better user experience through the application of chat bots in call centers, more effective diagnosis of health maladies through image recognition (think advanced detection of cancer),

The National AI Research Institutes are a vital first step toward ensuring U.S. leadership in AI – and by extension, ensuring our country’s economic future.

or fraud and spam detection, given the overwhelming amount of suspicious emails that are simply too much for any team of humans to take on.

But there are also real risks to consider, beyond the many we hear and read about, such as bias in data collection leading to outcomes that often disproportionately affect at-risk populations. There is also a set of counterintelligence (CI) risks. I'm in no way an expert, but I have had the opportunity to learn at a high level from cyber and CI experts while I was a Presidential Innovation Fellow detailed to the Federal Bureau of Investigations. So, I will briefly touch on a couple. The first is that cutting edge AI companies are highly targeted by hostile actors such as nation states because those technologies promise a technological, and therefore, an economic advantage on the world stage. And given that the U.S. government will make significant investments through AI acquisition, it's important for these companies and the government to ensure that these products and teams are not compromised in a way that could result in theft or hack of sensitive information in a government context.

Many experts would argue that it is impossible to fully mitigate the CI threat. So, it is also important that agency leaders and others responsible for mitigating such threats understand a second risk: how AI can be used if a hostile actor were to capture a wide swath of sensitive information (think the Office of Personnel Management hack). AI technologies can be used to understand the patterns and relationships in large amounts of data, i.e. in the case of the OPM hack, AI technologies can infer and build a deeper understanding of the behaviors of U.S. government officials whose information was compromised.

What this means is that the U.S. government must do more to mitigate the CI threat, which includes our cybersecurity posture. At the same time, it's also important not to lose sight of the bigger picture that represents the benefits of AI now and in the long term. Clearly, the risk calculus is challenging, but the U.S. government and our industry partners simply must continue to invest in AI technologies to maintain a competitive advantage and ensure the long term prosperity of the United States.

Developing OPSEC Expertise

*Wendy Elder,
ISD, Interagency OPSEC Support Staff (IOSS)*

The signing of the National Presidential Security Memorandum in January expanded the scope and requirements for operations security (OPSEC) programs, leaving many seeking resources and assistance for personnel and program development.

One approach to professional learning and development is the 70-20-10 model. The 70-20-10 formula describes optimal sources of learning by successful managers with 70 percent of learning gained through work experiences, 20 percent gained through interactions with others, and finally 10 percent gained through formal training and education.

To assist with 30 percent of the equation, the Interagency OPSEC Support Staff (IOSS) offers training and consultation services to help prepare and guide practitioners in creating and maintaining OPSEC programs.



National Counterintelligence Task Force

The National Counterintelligence Task Force (NCITF) hosted a **Women in Counterintelligence Leadership Forum** at the Applied Research Laboratory for Intelligence and Security on **June 29, 2021**. A panel of Senior Executive Service CI leaders from the Naval Criminal Investigative Services, National Geospatial-Intelligence Agency, and the National Counterintelligence and Security Center provided future leaders in the CI field with practical guidance and strategies to manage their careers and efficient tactics on leading others. The opening remarks were provided by FBI EEO AD and the closing remarks were delivered by Office of the Director of National Intelligence (ODNI) Chief of EEO and Diversity.

Additionally, NCITF and the FBI's Counterintelligence Training Center (CITC) hosted its second iteration of the **Introduction to Counterintelligence** training session. CITC and NCITF developed a four-hour course that provided an overview of the FBI's CI program, multiple in-depth CI case studies, and the CI program from the perspective of the Central Intelligence Agency. The second iteration of Introduction to Counterintelligence training session had more than a 50 percent increase of participation from federal agencies compared to the first iteration. As NCITF continues to provide training to our wide array of partners across the nation, we want to ensure trainings are beneficial and want to hear topics you would like to see covered in future training sessions; therefore, please send suggestions to FBI_NCITF@FBI.GOV.

Background of NCITF: The NCITF was established in October 2019 as a component of FBI's CI Division. The NCITF is responsible for supporting individual field offices Counterintelligence Task Forces (CITFs); ensuring multiagency collaboration, integration, and sharing; serving the CITFs as a national-level point of contact for component



agencies and leading CI campaigns. The NCITF is committed to ensuring the whole-of-government approach remains fully capable of conducting CI matters with a diverse, agile, and well-led workforce.

The Counterintelligence Implications of Neural Language Models

*Adam Jungdahl,
Research Faculty and Co-Director, Data Science
Intelligence Center, National Intelligence University*

The past few years have seen significant advances in AI technology. One particularly active area is in natural language processing, specifically the use of neural networks (i.e. deep learning) to analyze and generate original text. The largest and most capable of these neural language models, such as Google's XLNet or OpenAI's GPT-3, are trained on billions of words drawn from digitized libraries and scraped from the internet. With proper calibration, these models can produce original narrative text nearly indistinguishable from that of human authors. Today, the quality of the generated text tends to decline after the first few sentences. But in the not-too-distant future, one can expect to see longer, multi-page documents of original text composed and edited entirely by neural networks.

The evolution of neural language modeling offers many potential threats to U.S. national security. For instance, a recent study at Georgetown University demonstrated that a neural language model could generate an array of convincing tweets



containing misinformation across a range of subjects with little or no human intervention. Such a model could be used to generate a virtually endless stream of false or misleading online content. Similarly, a model trained to mimic an individual's writing style could be used to impersonate them in written communications. Such an approach could be used in email phishing attacks, as a means of identity theft, or simply to cause confusion and disruption within an organization. There are innumerable other potential malicious applications that, unfortunately, will only continue to evolve with the technology.

NCSC Special Security Directorate Overview

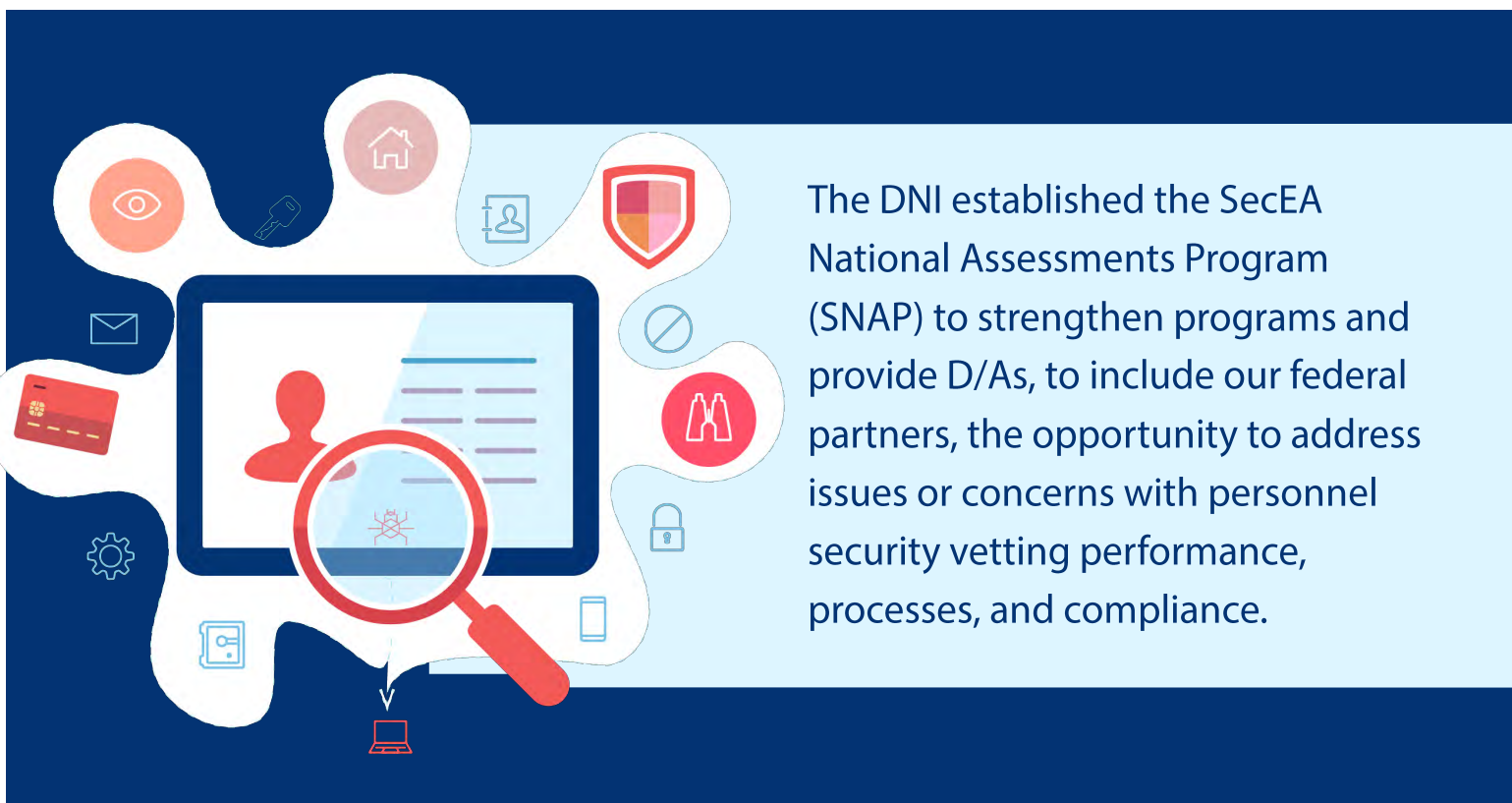
The NCSC Special Security Directorate - SecEA National Assessments Program (SNAP).

NCSC's Special Security Directorate (SSD) professionals serve as the Executive Staff for the Director of National Intelligence (DNI) as Security Executive Agent (SecEA). The 50 U.S. Code §3162a, and Presidential Executive Order EO 13467, as amended, assigns the DNI responsibility for effective and uniform policies and procedures governing access to classified information for the Intelligence Community (IC) and government-wide. SSD serves as the Executive Staff for all SecEA functions and responsibilities on behalf of the DNI.

To perform SecEA oversight responsibilities, the DNI established the SecEA National Assessments Program (SNAP) to strengthen programs and provide Departments and Agencies to include our federal partners, the opportunity to address issues or concerns with personnel security vetting performance, processes, and compliance. The SNAP program review is intended to supplement organization's existing internal oversight mechanisms. SNAP was established to ensure the quality, integrity and health of agency national security vetting programs by conducting oversight and compliance of business processes government-wide. SNAP assessors provide an overview of agency successes and areas of improvement, and make recommendations to strengthen national security programs. Additionally, SNAP assessor's measure agency performance against enterprise goals and baseline performance measures related to suitability and security reform efforts.

The Suitability and Security Clearance Performance Accountability Council is responsible to the President for driving implementation of the Security and Suitability Reform Effort and for ensuring accountability by agencies, ensuring the Suitability Executive Agent and the SecEA align their respective processes, and sustaining reform momentum.

For more information, inquiries should be directed to email: SNAP@dni.gov or SecEA@dni.gov.



The DNI established the SecEA National Assessments Program (SNAP) to strengthen programs and provide D/As, to include our federal partners, the opportunity to address issues or concerns with personnel security vetting performance, processes, and compliance.



NCSC Updates

Vera S.
Acting Group Chief, NCSC FPG

◆ FEDERAL PARTNERS MONTH ACTIVITIES

The NCSC designated May as Federal Partners Month. As stated by the Acting Director of NCSC in his Memorandum dated 17 May 2021, “Federal Partners Month reaffirms our commitment to work collaboratively with Executive Branch departments and agencies to detect, deter, and mitigate threats by increasing awareness and promoting a whole-of-nation effort.” In May, we issued a special edition newsletter, featuring articles from some of our federal partners. We also held a virtual quarterly CI roundtable with speakers who talked about AI and about the National OPSEC Program (NOP). If you follow NCSC on Twitter, you may have seen our tweets last month.

◆ OPSEC UPDATE

The NOP is preparing a starter kit for federal partners. The kit includes National Security Presidential Memorandum-28 language, a minimum standards checklist, frequently asked questions, and a summary of the NOP. These tools will help federal partners develop or refine their OPSEC programs.

◆ FEDERAL PARTNER COLLABORATION

We are pleased that federal partners have registered for accounts on the Structured Analytic Gateway for Expertise (SAGE) collaboration site. NCSC has posted numerous documents, videos, and event announcements that we hope are useful to you. The site is intended to encourage collaboration. Anyone who is a member of the ODNI NCSC Federal Partners Group space on SAGE has the ability to create posts; if you have information you would like to share with the federal partner community or have questions you would like to pose, please feel free to participate. If you have a specific collaboration request or question, use the “Ask ODNI NCSC Federal Partners Group” feature. Anyone member can respond to the unanswered questions. Additionally, to highlight specific focus areas, NCSC created a project in SAGE. You can access this project from the ODNI NCSC Federal Partners Group space. If you have questions please contact us at ncsc_fed@dni.gov.




Counterintelligence and Security Talent Development Working Group



The National Counterintelligence and Security Center (NCSC) Counterintelligence (CI) and Security Talent Development Working Group (CIS-TDWG) is charged with advising and assisting the Director, NCSC in developing standards and best practices to build and professionalize a highly skilled, agile CI and security workforce through advocacy, professional development, and community recognition initiatives. The CIS-TDWG is interested in your input.

Please send an email to ncsc_feds@dni.gov describing your top CI training and education issues and needs.

National Intelligence University Degree and Certificate Programs

 The National Intelligence University (NIU) offers bachelor and master degree programs as well as graduate certificate programs, including a degree concentration and a certificate in counterintelligence. All prospective students must meet the following eligibility criteria:

- ◆ Be a U.S. citizen;
- ◆ Be a member of the U.S. Armed Forces or a federal government employee; and
- ◆ Hold an active TS/SCI clearance.

//

NIU has additional requirements for applicants to the Bachelor of Science in Intelligence, Master of Science of Strategic Intelligence (MSSI), Master of Science and Technology Intelligence (MSTI), and Graduate Certificate and Continuing Education programs.

These criteria and descriptions of the programs are detailed at <https://ni-u.edu/wp/>.

Individuals interested in attending NIU programs should check with their organizational points of contact for information about how and when to apply for a nomination. Deadlines for upcoming programs are:

Spring 2021

Space-Available and Continuing Education - November 15, 2021

Fall 2022

Organizational Nominations Due for Full-time Study in Academic Year 2022-2023 - January 31, 2022

Part-time MSSI and MSTI Degree (All formats) - March 31, 2022

See events in SAGE for links



OPSEC COURSES

OPSEC Fundamentals (OPSE-1301)

WHEN
Self-paced online

REGISTER
Available at www.ioss.gov

OPSEC Analysis Course (OPSE 2380)

WHEN
17-18 August | 15-16 September | 19-20 October

Program Management Course (OPSE-2390)

WHEN
19 August | 17 September | 21 October

OPSEC and Public Release Decisions (OPSE-1500)

WHEN
27 July | 10 August | 25 August | 14 September |
28 September | 14 October

OPSEC and the Internet (OPSE-3500)

WHEN
11 August | 15-16 September | 6 October

Access these resources and more at www.ioss.gov
Interagency OPSEC Support Staff:
IOSS@radium.ncsc.mil or (443) 479-4677



TRAINING AND EDUCATION OPPORTUNITIES!

Personnel Security Adjudications Course (PSAC)

PURPOSE

This curriculum prepares security specialists to conduct adjudications of covered individuals to determine eligibility for initial or continued access to classified national security information or eligibility to hold a sensitive position in accordance with Intelligence Community Directive (ICD) 704 and Security Executive Agent Directive (SEAD) 4 guidelines. This program is also essential for security specialists from other security disciplines who need to better understand how their work directly supports national security eligibility determinations.

WHEN

30 August - 3 September 2021; OR
13-17 September 2021;
4 hours per day (AM or PM)

WHERE

Virtual instructor led via Webex

REGISTER

Please contact NCSC-Training@dni.gov to register.
There is limited seating for this event.

Sensitive Compartmented Information Facility Course (SCIF)

PURPOSE

This course will give you a better understanding of Intelligence Community (IC) physical security policies and prepare you to implement the requirements of the IC 705 series documents (ICD 705; ICS 705-1; ICS 705-2 and the ICD 705 Technical Specifications). The program also stresses the Life Cycle of a SCIF; design, construction, best practices and operations for a SCIF from cradle to grave and includes a security panel forum comprised of representatives from several IC elements Accreditation Offices.

WHEN

20-24 September 2021; 4 hours per day (AM or PM)

WHERE

Virtual instructor led via Webex

REGISTER

Please contact NCSC-Training@dni.gov to register.
There is limited seating for this event.

NITTF HUB Courses

PURPOSE

This course introduces the basic functions of an insider threat program's centrally managed analysis and response capability to gather, integrate, analyze, and respond to potential insider threat information derived from counterintelligence, security, information assurance, human resources, law enforcement, and other internal and external sources. scenarios.

WHEN

August 10 – 11, Registration opens July 1, 2021
September 14 – 15, Registration opens August 2, 2021

WHERE

Virtual instructor led via Webex

REGISTER

Insider Threat Program Managers or Senior Designated Officials must submit nominations via email to NITTF_Training@dni.gov with a nominee name, email address, department or agency name, and requested class dates. Classes fill quickly; submit nominations on or shortly after registration opening dates.



From the Acting Director



Michael J. Orlando
Acting NCSC Director

Over the coming month NCSC plans to prioritize for outreach and engagement several emerging U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the near future. The transformative technologies include AI, quantum information science, the bio-economy semiconductors, and unmanned systems.

In recent weeks, NCSC has been speaking to experts in and out of government to map out key aspects of the transformative technology landscape and leverage expertise as we embark on this outreach effort. Our outreach will be designed to raise awareness of nation-state threats to these sectors and help them protect their human talent and cutting-edge research from foreign exploitation.

As mandated by Congress, a core mission of NCSC is to conduct counterintelligence outreach to the private sector, the academic/research community, and other external stakeholders to arm them with information about foreign intelligence threats to their organizations. As you know, we routinely work with our federal partners in conducting such outreach to stakeholders and we look forward to partnering with many of you as we move forward in this venture.

Follow us on **Twitter** @NCSCgov to see the NCSC FPG's Defensive CI Tip of the Week for Federal Partners Month. For more information on NCSC CI and security topics, please visit our website at <https://www.NCSC.gov>. For questions about support and information available to Federal Partners, please email FPG at NCSC_FEDS@odni.gov.

“National Counterintelligence and Security Center (NCSC) plans to prioritize for outreach and engagement several emerging U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security”

Michael J. Orlando

