John Lindsay

Strategic Security Engagement, OpenAI

John Lindsay is a member of OpenAI's Global Affairs team, focused on Strategic Security Engagement. He works across OpenAI and with governments, academia, and the wider security community to bring geopolitical, regulatory, and strategic context to questions of security, resilience, and emerging technology risk.

Prior to joining OpenAI, John advised business leaders on cyber, digital, and geopolitical risk. Before this, he held national security and diplomatic roles across the UK government. His work has spanned nation-state cyber threats, insider risk and international affairs. He also has a technical background in penetration testing and exploit development.

Kyla Guru

Cyber Threats Policy Manager, Anthropic

Kyla Guru is Cyber Threats Policy Manager at Anthropic, where she architects safety mitigations for AI agents and LLMs before public deployment, tracks cyber misuse patterns, and leads pre-deployment safety evaluations. Her mission: ensuring AI systems are secure by design, not afterthought.

A Stanford-trained computer scientist (BS/MS), Kyla brings battle-tested expertise from offensive security and threat intelligence roles at SpaceX, Apple, MS-ISAC, and the U.S. Government. At Stanford, her thesis pioneered using LLMs for threat actor attribution and technique identification--research that now directly informs her work securing frontier AI systems. Beyond being a technologist, Kyla is a grassroots entrepreneur, reshaping cybersecurity education as Founder/CEO of the 501(c)(3) Bits N' Bytes Cybersecurity Education Corp. and co-founder of GirlCon Conference, which unites 700+ industry professionals and students annually to close tech's gender gap. Now in its 9th year, GirlCon has become the premier tech conference for high school students globally. A sought-after voice on AI safety and cybersecurity, Kyla has delivered keynotes at TEDxChicago, RSA Conference (USA and Singapore), and Tableau Conference, advocating for people-first security solutions. Her unique perspective—spanning nation-state threats to AI safety—positions her at the forefront of defining how we build, deploy, and defend AI systems in an increasingly complex threat landscape.

Jonathan Snow

Deputy Director, Homeland Security at Cal OES

Deputy Director Snow was appointed by Governor Newsom and joined the California Governor's Office of Emergency Services (Cal OES) in August 2024. Deputy Director Snow provides direction and oversight to the Cal OES Homeland Security Division. In this role, Deputy Director Snow is responsible for the State Threat Assessment System (STAS), the California Cyber Security Integration Center (Cal-CSIC), and the following homeland security programs: the Governor's Homeland Security Advisory Committee; the Governor's Cybersecurity Task Force; Port and Maritime Security; Chemical Biological, Radiological, Nuclear and Explosive material (CBRNE) Protection and Preparedness; Event Planning Security; Critical Infrastructure Protection; and Statewide School Safety. Moreover, Deputy Director Snow provides administrative oversight to the application of California's homeland security grants, known as the Homeland Security Grant Program (HSGP) and Urban Area Security Initiative (UASI).

Prior to joining Cal OES, Deputy Director Snow spent 21 years with the Federal Bureau of Investigation (FBI) as Special Agent, specializing in national security threat issues. Assigned to the Sacramento Field Office, his final assignment at the FBI was an executive management role as the Assistant Special Agent in Charge (ASAC) overseeing the National Security and Crisis management programs, where his responsibilities included International and Domestic Terrorism, Counterintelligence, Cyber, Critical Incident Response, SWAT, Training, National Academy, and Division Compliance/Chief Security Officer. Deputy Director Snow also spent over three years in Washington, D.C. as Supervisory Special Agent with the FBI's Counterintelligence Division.

Thomas MacLellan

Director, Government Affairs and Strategy at Palo Alto Networks

Thomas MacLellan leads Palo Alto Networks' state and local government affairs practice. In this capacity, his role is to educate policymakers on current and emerging cybersecurity threats, national and international trends, and strategic policy opportunities to improve defenses.

Thomas has over 20 years of experience working nationally on a range of issues including cybersecurity, homeland security, disaster response, public safety broadband, and digital privacy. He has led government affairs for two multinational cybersecurity companies and was Director of Homeland Security, Technology, and Public Safety for the National Governors Association (NGA). At NGA, Thomas led the Governors Homeland Security Advisors Council (GHSAC) and created the first national effort to improve state cybersecurity. Thomas also staffed the Council of Governors and led a national effort to help states implement FirstNet. In each of these roles, Thomas regularly worked with senior homeland security and public safety officials, federal agencies, the White House, and Congress.

Thomas has trained governors and other C-Suite executives on disaster response and has worked closely with DHS, FCC, DOJ, FEMA, HHS, and DoD. He has published numerous articles and served on multiple federal and state advisory councils. Thomas is a graduate of the College of the Holy Cross and the Center for Homeland Defense & Security at the Naval Postgraduate School in Monterey. He also earned an Executive Certificate from Harvard University on mitigating cybersecurity risks and was named by StateScoop as a Top Industry Leader.

Dr. Nate Gleason

Program Leader for Cyber and Infrastructure Resilience, Lawrence Livermore National Laboratory

Dr. Nate Gleason is the Program Leader for Cyber and Infrastructure Resilience (CIR) within the Energy and Homeland Security Program in the Global Security Directorate at Lawrence Livermore National Laboratory (LLNL).

Dr. Gleason joined LLNL as the founding Program Leader for CIR in January 2016 and has since helped the program grow to several hundred technical staff. The Cyber and Infrastructure Resilience Program is focused on providing the nation with the capabilities to compete in “gray zone” conflict space. A major portion of this involves assuring the resilience of the nation’s critical infrastructure by enabling a future where our critical infrastructure systems are intelligent, self-healing, and resilient to cyber and physical disruptions. CIR also works to enable American leadership in energy by helping to create a modern, secure and reliable electric grid that incorporates a diverse set of energy sources. Key sponsors for this program include the Department of Homeland Security, Department of Energy, Department of Defense, and the State of California.

Prior to joining LLNL in January 2016, Dr. Gleason spent 12 years at Sandia National Laboratories in a variety of technical and management positions including Deputy to the Vice President, Deputy Program Director for Sandia’s Homeland Security Program, Department Manager for the Advanced Systems Engineering and Deployment Department and Department Manager for the Systems Research and Analysis Department.

Dr. Gleason completed his undergraduate work at the Massachusetts Institute of Technology, and received his Ph.D. from Princeton University.