CYBER-AI CONVERGENCE WORKING GROUP CHARTER

Mission Statement

The Cyber–AI Convergence Working Group advances the secure, responsible, and operational integration of artificial intelligence and cybersecurity across government and industry. The group's mission is to strengthen national digital resilience by ensuring AI-enabled systems are cyber-secure by design, while leveraging AI to enhance the speed, scale, and effectiveness of cyber defense.

Context

Cybersecurity and artificial intelligence are converging from parallel disciplines into a shared operational reality. Adversaries increasingly employ automation, AI-enabled reconnaissance, and machine-speed attacks that overwhelm human-centric defenses. At the same time, organizations are rapidly deploying AI systems that introduce new attack surfaces, governance challenges, and systemic risks.

Roundtable participants from government, industry, and academia emphasized that this convergence is already underway and unavoidable. AI is becoming essential to cyber operations, while cybersecurity must now account for protecting AI systems themselves—including models, data pipelines, agentic workflows, and integrations with third-party services.

A consistent theme emerging from the discussion was that success in cyber–AI convergence will depend less on model sophistication and more on governance, data discipline, operational integration, continuous risk management, and sustained human judgment. The working group is established to move beyond experimentation toward practical, mission-ready implementation.

Scope

The working group will address cyber–AI convergence as an integrated operational challenge, encompassing both AI for cybersecurity and cybersecurity for AI. The scope emphasizes real-world applicability, risk-informed decision-making, and outcomes that support federal missions and critical infrastructure.

Objective

- Examine how AI can be applied responsibly to cyber defense functions such as threat detection, incident response, testing, and continuous authorization.
- Identify and address cybersecurity risks unique to AI systems, including data integrity, model exploitation, agentic behavior, and supply-chain dependencies.
- Advance governance approaches that move beyond static compliance toward continuous, risk-based assurance.
- Promote data strategies that prioritize quality, provenance, relevance, and lifecycle management over indiscriminate scale.
- Support workforce readiness by fostering AI literacy among cyber professionals and security awareness among AI practitioners.

- Enable cross-sector collaboration among government, industry, and academia to align practices and reduce fragmentation.

Deliverables

The working group will produce practical, action-oriented outputs, which may include:

- White papers and briefs outlining operational best practices for cyber–AI integration.
- Frameworks or guidance for securing AI systems as critical cyber infrastructure.
- Use-case analyses highlighting effective and constrained applications of AI in cybersecurity operations.
- Recommendations for data governance, continuous authorization, and assurance models relevant to AI-enabled systems.
- Workshops, roundtables, or webinars to share findings and support implementation across the community.

Working Group Membership

Working Group Chairs

Martin Stanley, NIST , Government Chair - Pending Agency Approval
Scott Orton, Owl Cyber Defense , Industry Chair

Working Group Chairs will:

- Attend and contribute to each Working Group meeting
- Prepare the meeting agenda, solicit topics for discussion, assign members to address discussion topics, and distribute meeting materials
- Share information of relevance; provide an update/introduction at the beginning of each meeting to encourage member engagement
- Define and oversee Working Group initiatives and activities
- Assist in all stages of the deliverable production process
- Advocate for government, academic, and industry involvement in the working group
- Referee requests and suggestions for working group membership regarding agenda, deliverables, and representation

Working Group Members

Group members are strictly voluntary, and we strive for a broad representation across government, private sector, and academia.

Working Group Members will:

- Participate in meetings, including exchanging technical information, experiences, and best practices to develop a shared understanding of the topic(s) discussed
- Gather information and work on group deliverables outside of meetings as needed
- Provide feedback on draft deliverables as requested
- Co-lead or participate in Sub-Working Groups (breakout teams/project teams) as needed
- Provide input on meeting agendas as requested

ATARC Support

Elizabeth Wyckoff, Associate Director, Working Groups
Amy Karpowicz, Working Groups Associate
Taylor Gibbs, Working Groups Associate

ATARC support will:

- Serve as program management for the Working Group
- Coordinate and drive group projects and deliverables forward
- Schedule Working Group meetings
- Develop Working Group meeting agendas along with the chairs
- Facilitate Working Group meetings along with the chairs
- Assist in distributing relevant documents and materials to Working Group members
- Record meeting minutes, post-meeting decisions, and action items, and distribute them to Working Group members after each meeting
- Assist in preparing final proposals/recommendations
- Provide marketing services for the Working Group (promoting completed deliverables, etc.)
- Develop strategies to improve Working Group engagement, including applicable cross-overs with other Working Groups and relevant events
- Coordinate Working Group Labs as applicable

Rules of Engagement

The Working Group rules of engagement are described as below:

- Meet bi-weekly from 2026 to 2027, or until amended by ATARC Support
- Join Working Group meetings prepared and with requested action items completed
- Provide respectful and constructive feedback to yield the best decisions for the Working Group's objectives
- Endeavour to balance time among members so that all may contribute. All members of the Working Group have a voice and will be listened to.
- Final decisions are made by the Working Group Co-Chairs and ATARC Support
- If a Working Group member misses a meeting, decisions will be made in their absence. The Working Group will consider on a case-by-case basis at the request of the absentee if a decision made in the absence of a member shall be revisited.

-

The Working Group will:

- Meet every other Thursday from 1:30 - 2:30 PM EST.
- Form Sub-Working Groups (breakout teams/project teams) as needed
- Follow the group's ground rules as developed in the charter
- Meet critical deadlines in the creation of deliverables by mutual and balanced effort
- Keep in confidence draft versions of deliverable, off-the-record conversations, and non-public Working Group or ATARC plans to the extent disclosure is not required by law, regulation, or valid court order

File Sharing and Collaboration Tools

Access to the ATARC Box Account is managed by ATARC Support.

Disclaimer: Products and communications by ATARC's Cyber-AI Convergence Working Group do not necessarily represent the plans or preferences of any company or government agency.