# Trusted AI Agents Working Group Operating Addendum

This Working Group Operating Charter extends the Scope and details the related requirements and operational processes important for the Working Group's operation. This document is not legally binding but once approved by the Working Group it provides additional requirements for the Working Group.

1. Working Group Name. **Trusted AI Agents Working Group**

2. Operations and Duties

Initial chairs include:

- Nicola Gallo
- Andor Kesselman
- Dmitri Zagidulin

3. Participation

We welcome contributions from:

- Spec authors and security researchers
- LLM infrastructure and agent-framework maintainers
- Identity & authorization experts

4. Initial Work Item: Agentic Authority Use Cases

Evaluate existing object capability-based mechanisms and, where necessary, propose a streamlined specification tailored to AI agent workflows.

5. Possible Future Work Items (examples, not limited to)

- **Discovery**: Align with NANDA's AgentFacts and evaluate the NANDA Index to define protocols and registries for agent discovery and service advertisement.
- **Agent-to-Agent Messaging** : Work with ToIP and other specifications to deliver secure, trust-preserving communication patterns between autonomous agents.:
- **State Management**: Interoperable formats and storage models for agent state checkpoints and snapshots.
- **Interaction Interoperability:** Schemas and APIs for consistent agent interaction patterns (e.g., tool invocation, human handoffs).
- **Additional Capability Profiles**
  Extensions of O-Caps-AI for specialized domains (e.g., data marketplaces, IoT control, policy authoring).