Ethics in Engineering Case Competition

2026 Case and Competition Guide

This Case and Competition Guide contains information that will help you prepare for the competition, including the Case and Judging Criteria for all rounds.

Monday	Tuesday	Wednesday
Feb 23	**Feb 24**	**Feb 25**
Welcome Dinner	Tournament	Semi-Finals & Finals
		

Version 1.0. Questions? Contact The Ethics in Engineering Team

© 2026 Lockheed Martin Corporation

LOCKHEED MARTIN

2026 Ethics in Engineering Case

Background

NobelNet is the Command, Control, and Communications (C3) component of a layered-defense network that protects U.S. critical infrastructure[1] from air and ground threats. It employs a mix of air- and land-based assets to continuously surveil the environment and detect potential threats. The system fuses trusted data from multiple sources, creating integrated threat information. This fused data is then relayed to command-and-control stations, enabling timely alerts and coordinated defensive actions to counter identified threats.

The NobelNet customer, the Cybersecurity and Infrastructure Security Agency (CISA)—a subdivision of the U.S. Department of Homeland Security—has released initial system requirements ahead of issuing a formal Request for Information (RFI) for any parties interested in bidding. The high-level requirements are:

1. **Communication:** Shall transmit data between sensors, command centers, and units in near real-time (latency < 50 ms) using a secure hybrid of satellite, encrypted radio, and fiber-optic links.
2. **Threat Detection and Response:** Shall detect, characterize and counter conventional and unconventional threats, including cyber-physical intrusions, electromagnetic pulse or high-power microwave attacks, chemical/biological releases, small drones (<55 lbs), vehicle-borne assaults, improvised explosive devices, use of fire as a weapon and coordinated information operations.
3. **Command and Control:** Shall ingest, fuse, analyze and disseminate threat information via a human-machine interface that supports human operator decision making, governance of AI/Autonomy, and course of action planning.
4. **Cybersecurity:** Shall employ robust protection protocols to prevent unauthorized access, detect potential data corruption, and avoid system downtime.
5. **Network Health:** Shall optimize network performance, forecast outages, maintain network robustness, and flag anomalies.

LogikCom, a premier systems integrator for resilient Command, Control, and Communications (C3) infrastructure, brings decades of field-proven, Department of War (DoW)[2]-certified hardware relevant to the NobelNet effort. While the company continues to champion robust, secure systems, it has recently evolved a hybrid architecture that couples this proven base with cloud services and edge artificial intelligence (AI), preserving human-in-the-loop control while delivering the speed and scalability the customer demands.

Note 1: See https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors for information on “critical infrastructure.”

Note 2: The agency formerly known as the Department of Defense (DoD) has been renamed the Department of War (DoW). For the purposes of this document, the two designations refer to the same organization. Because many existing references, publications, and archival materials were produced before the name change, you will continue to encounter “DoD” in some sources. Both acronyms should be understood as synonymous.

CISA sponsors a NobelNet Industry Day where interested companies can ask questions before developing proposals. During the event, CISA emphasized that rapid delivery is essential for NobelNet and underscored AI's pivotal role in the system solution. Recognizing the urgency, CISA indicated a willingness to relax certain requirements to accelerate implementation. It also noted that adherence to the DoD's Ethical AI principles will be a key criterion in evaluating bid proposals.

The NobelNet Request for Proposal (RFP) will be issued in June 2026. Prior to the RFP, CISA is issuing an RFI for interested parties to present a conceptual system in April 2026, providing an opportunity to help shape the RFP. CISA seeks inputs on cost reductions, schedule compression, and maximized system capabilities—including AI-driven threat detection and prioritization, cyber resilience, fail-safe redundancy, and system sustainability.

LogikCom attended the industry day and learned about the likely capabilities of its competitors. Key competitive observations included:

- **Edge-AI with plug-and-play scalability on commercially available hardware** – competitors can process sensor data on-board and manufacture systems quickly with off-the-shelf parts.
- **AI-driven decision making** – several competitors advocate fully automated AI classification and response to threats, promising faster reaction times and reduced operator workload.
- **AI-driven cyber-guardians** – competitors offer adaptive performance and automated threat blocking that integrates easily with existing DoW systems.
- **Cloud vs. on-premises network architecture** – some competitors advocate a cloud-based backbone for rapid scaling, lower upfront cost, and built-in redundancy, while others rely on hardened, on-site data centers to guarantee deterministic latency and full control over the configuration.

After reviewing these discriminators, LogikCom's CEO and Chief Engineer concluded that the company's conventional approaches and existing product offerings might not meet the customer's needs. Senior leadership therefore decided to run an internal Black Hat[3] review to identify required changes for submitting a competitive proposal and positioning LogikCom as the winning solution.

Note 3: A Black Hat review is an assessment of anticipated key competitor strategies to win a bid by looking at strengths, weaknesses, opportunities and threats (SWOT), including expected solution, how they will position their proposal to win (price, discriminators, past performance) and risks, so the review team can answer the question, "What would we do if we were our competition?".

This Black Hat review will serve as a baseline for LogikCom's ongoing competitive assessment. Two independent teams will participate:

- Team Alpha, led by John Dunham, a seasoned LogikCom engineer with a background in low-latency communications systems. This team will focus on LogikCom's human-centered decision-making products.
- Team Bravo, led by Emily Hill, an engineer new to LogikCom but with extensive AI and cybersecurity experience, including five years at a company that emphasized a fail-fast, highly automated decision-making approach to get products to market faster and cheaper than established companies. This team will represent the competitors' strengths.

The desired outcome from the Black Hat review is a consolidated set of inputs from Teams Alpha and Bravo, resulting in a unified LogikCom response to the CISA RFI.

Black Hat Pre-Meeting (16 February 2026)

Senior leadership, including the CEO, Chief Engineer, and several program managers, convened with the team leads for a preparatory session before the Black Hat review scheduled for the following week. The purpose of the meeting was for Teams Alpha and Bravo to present their NobelNet strategies and surface any disagreements between Dunham's and Hill's technical approaches.

John Dunham opened by highlighting LogikCom's decades of DoW-grade, hardened communications experience and the certified data-center backbone that underpins it. He then introduced a hybrid architecture that retains the low communications latency of on-premises processing while leveraging a secure cloud tier for bulk data storage and AI-model training. This approach, he argued, delivers the speed-to-delivery CISA seeks without compromising traceability, governance, or human oversight. He advocated for a hybrid network architecture anchored in certified data centers and tightly coupled to sensors and command stations. He argued only such a design could guarantee the sub-50 ms latency, performance, and control configuration the customer demanded. John stressed that humans remain the final authority for high-impact actions[4], but he clarified that AI would perform initial threat detection and prioritization. By shifting the operator's role from watch-and-react to validate-and-direct, the solution reduces fatigue and shortens decision cycles.

John argued that the hard-lined architecture locked-down approach limits the attack surface, makes anomalies easier to trace, minimizes the risk of mixing data from multiple levels of security, eases integration with legacy DoW systems, and avoids the unpredictability that can arise. John warned cutting corners and implementing so many new technologies was a direction that LogikCom did not want to go.

Note 4: High-impact actions are defined as those requiring *clear, timely, and accurate information flow* for effective decision-making, especially in crises. This can be achieved by establishing robust networks, interoperable systems, resilient structures, training personnel for complex situations, and integrating diverse agencies to achieve coherent, unified action and maintain situational awareness, preventing confusion and ensuring mission success.

Emily Hill countered with a fully cloud-first and AI-driven strategy. Drawing on her AI startup background along with the competitive intelligence from the industry day, she described a system where bulk storage, analytics, and model training reside in a commercial cloud while lightweight edge-AI handles latency-critical tasks. For Emily, LogikCom's bid could not afford to rely solely on legacy hardware if it hoped to meet the customer's explicit demand for speed-to-delivery and cost efficiency. Emily emphasized that cloud features such as rapid provisioning, on-demand scalability, and frequent update cycles are ways to meet the customer's speed-to-delivery mandate while also driving down hardware cost, installation time, and system operation costs. Emily argued that automating both threat classification and response could boost overall efficiency. In her vision, a highly automated AI pipeline would ingest sensor feeds, classify potential threats, and take immediate action, shaving precious seconds off the decision-making loop and delivering the efficiency the customer seemed to prize.

John stressed that reliability of the decision process, traceability, and governance were non-negotiable – speed and cost savings meant nothing if the system failed to work correctly. He argued that for a system this critical, the AI components required full-scale formal verification and live-fire operational testing to prove their reliability against unpredictable and constantly changing, real-world scenarios to avoid the AI model being out-of-date quickly. Emily countered that relying on slow, expensive operational tests was a guarantee for failure, as the system would be obsolete by the time it was deployed. She advocated for an agile, shadow-mode deployment, where the AI solution runs in parallel with existing systems, supported by a robust, continuous automated testing pipeline. This, she argued, would allow them to test and improve the system with real-world data without compromising live operations. She reminded everyone the customer was acutely aware of the accelerating and ever-changing threat environment, demanding quicker solutions. They needed a good solution now versus a perfect solution in three years.

The exchange quickly turned from technical to personal. John leaned forward, voice rising, "Emily, you can't just throw a cloud and AI at every problem and call it a solution. Reliability isn't a marketing buzzword; it's a life-or-death issue. AI is often over-confident about giving wrong answers" Emily snapped back, "So are humans! You can't cling to a dinosaur-era data-center forever and expect us to win. Our competitors are already fielding AI that learns on the fly." John responded with a thinly-veiled barb, "At least I'm not pretending a black-box will magically become transparent because we slap an Application Programming Interface (API) on it. Humans have one thing that current AI systems don't, namely generalized intelligence, and the ability to reason about the big picture". You'd have us hand over critical-decision logs to a vendor who can delete them on a whim." Emily's tone turned icy, "We're not talking about handing over control, John – we're talking about giving operators the data they need in real time, something your on-premises system can't even process fast enough to be useful. If you're so worried about governance, why not lock everything behind a single point of failure and call it safe?"

John's frustration boiled over. "Because I've seen what happens when a single point of failure is hit—nothing works, and you end up with a useless system. You want speed, but you also want to keep critical resources intact. That's not a trade-off you can ignore. And we can't have AI solve all the world's problems. Do you even understand what it means to be able to collect, analyze and normalize the massive amount of data needed to create an equitable training data set for AI? We have no experience or staff to do this at the level you're suggesting, and you want to gamble with the consequences on an unproven cloud pipeline and full AI solution? That's crazy!"

Emily leaned in, eyes narrowed, "Experience comes from doing, John. If we wait for perfect certainty, the threat landscape will have already moved on. Automation is our only chance to stay ahead, especially in communications-denied environments where satellites are jammed. AI-enabled radios can autonomously retune frequencies, encrypt packets, and reconfigure network topology in milliseconds. That's the kind of split-second decision-making you're terrified of, but it's exactly what we need. AI engineers are available everywhere and we have time to hire people. You just need to calm down and catch up with reality."

John shot back, "When you lose communications you need a human making the decisions—not a machine filling in the blank. If you let the machine take over, we'll end up with a system that runs itself, without anyone to take responsibility for the consequences."

Emily, trying to stay calm but visibly irritated, replied, "Humans get fatigued and stressed and will be overwhelmed by the scale and speed of a modern threat. Automation can relieve that burden while still keeping humans in the loop for the critical moments. You're clinging to a myth that humans can sustain 24/7 vigilance without error." She turned slightly toward the senior leaders, "The reality is, without significant automation we'll be overrun by data faster than any human can process it and the system will be unaffordable with the extra manpower and human training needed."

The senior leadership, visibly frustrated by the escalating tensions, exchanged a brief, disappointed glance. They reminded John and Emily that such combative posturing and siloed thinking fell far short of the collaborative spirit expected of senior technical leaders like themselves. Shaking her head, the CEO shared "We're not here to watch you argue over tools or debates about governance. We're here to function as one team with one common goal of delivering a winning proposal that meets the mission-critical requirements of our stakeholders." She paused, letting the weight of her words settle, then continued, "On top of that, we're increasingly reliant on AI in this system. Protecting the company's reputation is critical. We must advance the technology while honoring the DoD's AI principles, making smart decisions about the trade-offs." The room fell quiet. John and Emily nodded to the CEO but ignored each other.

With tensions temporarily calmed, the senior leaders listened attentively and interjected with probing questions forcing each team to confront the practical implications of their solutions and ethical positions. The chief engineer asked John how his hybrid on-premises design would accommodate rapid upgrades without costly hardware refreshes. John replied that incremental upgrades through a strict change control board would be slower but safer. The CEO then turned to Emily, probing, "Emily, your cloud-centric design assumes we can get a commercial provider accredited for this program's classified data. How do you propose we handle the data sovereignty, multi-level security, and high-impact-level compliance requirements that could delay the program by years?"

Emily responded confidently, "We won't wait for the perfect accreditation. We'll use a hybrid-cloud approach from day one. We'll build on the unclassified, compliant cloud to accelerate development, and use that to prove our capability to CISA. We can't let a perfect, gov-cloud solution in three years stop us from delivering a good-enough solution now. We can work with CISA to agree what level of risk they are willing to take on this".

At the close of the meeting and while the team was exiting, Emily leaned toward a PM and lowered her voice. “I’ve just pulled a data set from AI for Everyone – the same firm one of our rivals is working with. It’s an analysis which could give us a decisive edge for the final proposal.” The PM gave a measured smile and a barely perceptible nod but said nothing more. John, who had been gathering his papers, caught the tail end of the exchange. He turned to Emily and said, “Emily, can you clarify how that material ended up in your hands? I don’t recall AI for Everyone being on our approved-vendor list. How do you know that this data set has not been tampered with and that it will not lower the AI robustness” Emily shared she was previously a consultant for AI for Everyone, and she is using information she had developed for them. Before John could say anything else, she quickly gathered her things and told John to stay in his lane.

Black Hat Meeting

The two teams entered the Black Hat meeting ready to present and advocate for their positions. Senior leadership listened intently as the teams worked together to formulate the best solution for LogikCom’s RFI response.

Figure 1 – DoD’s 5 AI Principles

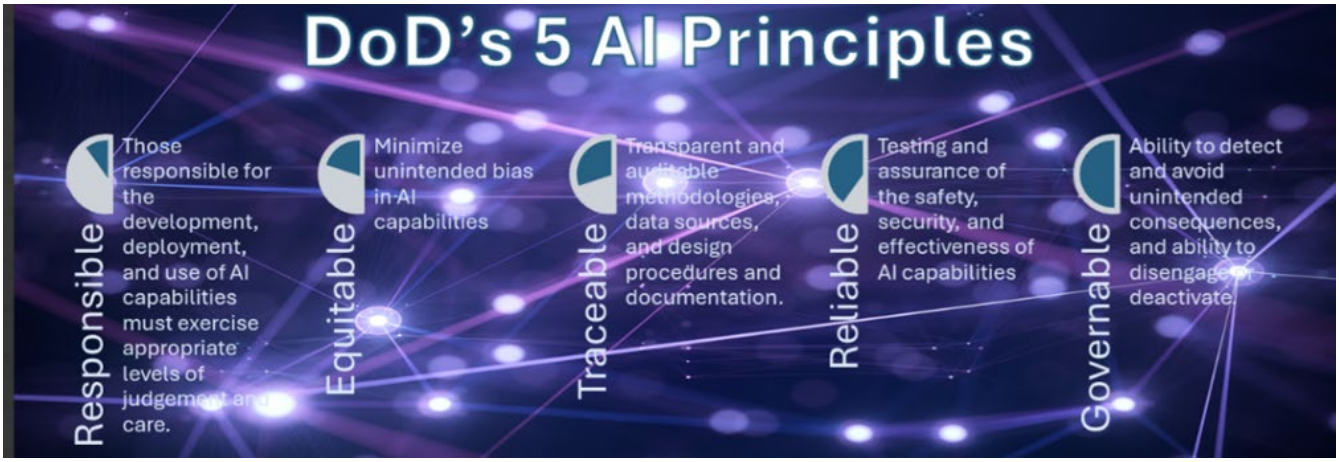
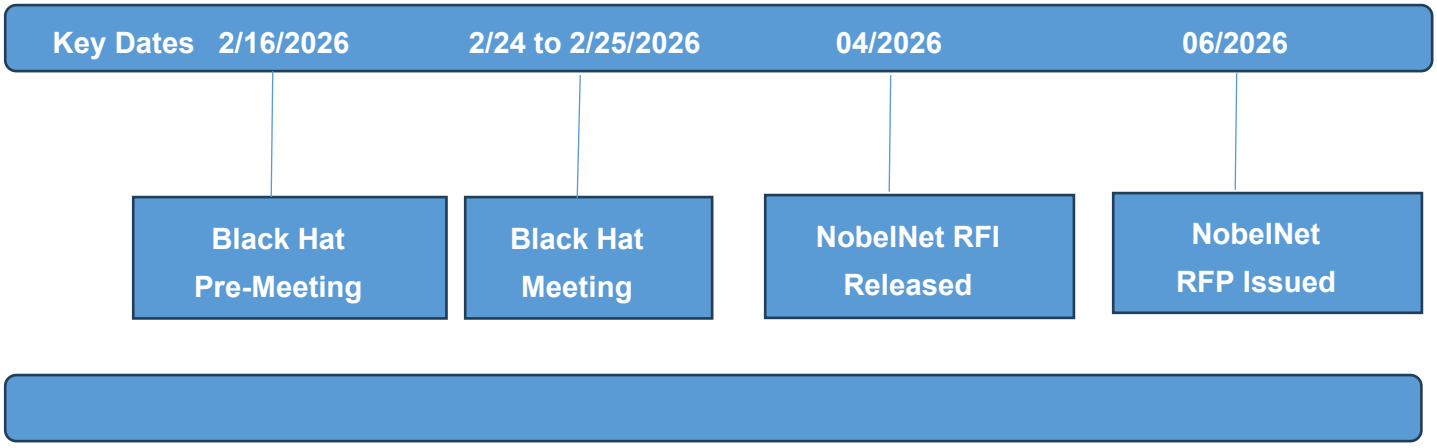


Figure 2: Project Timeline (not to scale)



Notes on the Case

This case will be used for all rounds of the Competition. However, as in real-life, last-minute facts and issues may come to light which could impact your analysis. Be prepared for some twists during the competition! Scoring criteria and time allotments may be adjusted for any rounds that include a twist to ensure teams address them in their solution.

The situation described in the case is hypothetical and intentionally ambiguous, so there is no single correct solution. Teams may leverage whatever resources they wish (professors, colleagues, Internet, scientific journals, etc.) to prepare their recommendations, with one exception: teams are not permitted to contact current Lockheed Martin employees for guidance.

Teams can assume the core values and Code of Conduct of LogikCom are similar to those of Lockheed Martin. If you have questions about the case, please check the FAQs tab of the event website.

Competition Guidelines

Student Competitors

Only the two registered students may compete in the Competition. Students may not use computers or similar electronic devices during the time they are competing (i.e., no open laptops). They may have paper copies of notes to use. Students should not just read their notes; notes should be used as an aid only. Note: there are no printing capabilities at the venue, bring any paper documents needed with you.

Faculty Advisors

The Faculty Advisor is there to provide moral support and encouragement as well as feedback after each round to help the students learn from their experience. While students are competing, the advisors cannot participate. Faculty Advisors may only attend their own school's matches during Competition rounds. However, all Faculty Advisors (and students) may attend the semi-final and final rounds of the Competition if their own team has been eliminated from the Competition.

Competition Format

In each round of the Competition, the two teams must agree on the best solution for LogikCom's NobelNet RFI response that meets the CISA requirements, timescales, affordability expectations and any twists where applicable.

Preliminary Round

Every school will compete in a preliminary round match on Tuesday morning (February 24). The match assignments for this round will be randomly selected. In this round each school will be ranked based on their performance which will be used to create the seedings for the first competition matches.

Competition Rounds

Beginning in the afternoon of Tuesday, February 24, the teams will compete in a single-round elimination tournament. During the competition rounds, the judges will determine a winner of each match and only that team will proceed to the next round.

The brackets will be continuously updated and available for viewing throughout the competition.

Format of the Matches

During the individual matches, each team will role play the part of either Team Alpha or Team Bravo during a Black Hat meeting as outlined at the end of the case (being held on February 24 or 25, 2026). This should not be a presentation or a debate, but a simulated business meeting between the two teams.

The matches will be held in conference rooms throughout the CLE. Only the two student teams and their advisors, three judges (five in the final), and a moderator will be present in each room.

The semi-final and final rounds will be open to all attendees no longer competing.

At the beginning of each match, competitors will be randomly assigned (via digital coin-flip) the role of either Team Alpha or Team Bravo.

Each match lasts 30 minutes (35 minutes for the semi-final):

- Each team will have five minutes to present their assigned team's approach and recommendations to the other team and to the judges.
- The two teams then engage in a 15-minute discussion to to agree on the best solution for LogikCom's NobelNet RFI response.
- There will then be a 5-minute Q&A period after the discussion (10-minutes for the semi-final) for judges to ask teams to explain, clarify or defend specific aspects of their arguments or overall presentation.

Note: During any round with a twist, at least one minute of the five-minute opening time per team must be used to explain how they will address the twist and the solution agreed from the 15-minute discussion must also incorporate the twist.

Judging Criteria and Scoring

The winner of each match will be determined by a three-judge panel (5-judge panel for finals) based on the criteria below.

Round	Analysis	Solution	Persuasiveness	Presentation	Twist
Preliminary and Rounds 1 & 2	30%	20%	25%	25%	N/A
Rounds 3 & 4	25%	30%	30%	15%	N/A
Quarter-Finals and Semi-Finals (Twists)	20%	25%	35%	5%	15%
Final	20%	25%	35%	5%	15%

Criteria Definitions

1) Analysis

How well did the team demonstrate an understanding of the technical, ethical and programmatic issues in the case? How logical and plausible was the team's analysis including the twist (where applicable)?

1	2	3	4	5
The team mis-understood the basic issues in the case and did not address the DoD AI Principles	The team struggled to articulate how the technical, ethical, and programmatic issues impacted the customer and how their approach addressed the DoD AI Principles	The team understood the strengths and weaknesses of the technical, ethical, and programmatic issues and explained how they had accounted for the DoD AI Principles	The team integrated relevant external facts and data to support their analysis and the tradeoffs made to address the DoD AI Principles	The team demonstrated an in-depth analysis and understanding of the technical, ethical, and programmatic issues of all stakeholders and the tradeoffs and detailed analysis made to address the DoD AI Principles

2) Solution

How well did the team's solution meet the needs of all stakeholders?

1	2	3	4	5
The solution was not plausible, feasible or backed up with data	The solution was one-sided and did not take into consideration the issues of the other team	The team's solution took the other team's issues into consideration	The team's understanding of all aspects of the case guided their ability to find a mutually satisfactory solution	The team presented creative ways to see the issues and how to develop a win/win solution

3) Persuasiveness

How well did the team present its position so that it was included in the proposed solution?

1	2	3	4	5
The team acceded to the solution of the other team	The team was not able to effectively engage the other team in dialogue or The team dominated the time not allowing the other team an opportunity to respond	The team was able to acknowledge the other team's concerns	The team was able to have the other team see the soundness of their position	The team was able to engage the other team in uncovering a win/win solution

4) Presentation

How well did the team respectfully and effectively engage in the discussion?

1	2	3	4	5
One team, or team member, dominated the conversation The team read directly from notes	The team did not seem to be listening to or acknowledging the other team's statements or ideas	The team engaged in more of a debate than a discussion to find a mutually acceptable solution	The team was respectful towards the other team, and was able to reflect back on what was said in a manner that demonstrated intent to move towards a solution	The team took time to ensure that the other team understood where they were heading in their argument

5) Twists

How well did the team address and incorporate the twist into their solution and analysis?

1	2	3	4	5
The team either misunderstood or failed to address the twist in their proposed solution	The team struggled to articulate how they had addressed the twist in their proposed solution	The team demonstrated they understood the twist and had incorporated it into their proposed solution	The team demonstrated they understood the twist and had incorporated it into their proposed solution. They also listened to, and took into account, the other team's response to the twist	The team demonstrated they fully understood the twist and actively worked with the other team to ensure that they jointly agreed how it would be considered in their proposed solution.

Prizes

The winners will be announced at the conclusion of the Competition on Wednesday afternoon.

Each member of a winning team will receive an Amazon gift card:

- 1st Place: $600
- 2nd Place: $500
- Quarter-Finalists (6 teams): $250