



/Abnormal

#49

Patricia Titus

Field Chief Information Security Officer

Abnormal AI

Public role source revisited. Employer/self sources and association/event biographies are distinguished; direct role acceptance is not established. **Current-role source**

Direct business email and telephone: not publicly verified.

LinkedIn profile | Named professional biography / public route

Work base: Not established from reviewed sources. Actual work base, DC access and willingness require direct confirmation.

Recommendation and rationale

Hold for title/remit qualification. Historical policy experience and current field CISO; establish operating responsibility and company-sponsored representation.

Research rank #49 - Sponsor / remit qualification. Final research recommendation for this pass; ISA selection and outreach approval pending.

Company capacity and proposed benefit

More than \$200m ARR reported August 2024, with \$250m Series D expected proceeds. Historical ARR and financing; not current audited revenue. **Source: abnormal.ai**

Proposed company benefit: Test Abnormal AI's useful vendor-neutral contribution; confirm field-CISO eligibility and payer.

Proposed executive benefit: Contribute her public AI governance and identity perspective.

What This Recruit Could Add to ISA

Develop an AI inventory case with accountable owners and human risk-acceptance decisions. **Source: abnormal.ai**

Handbook connection: Tool E 48-50. Proposed output and benefits require agreement. **Source: www.nacdonline.org**

Introduction and next decision

No named introducer established. ISA to designate an approved contact route; no private relationship inferred.

ISA to reconcile account status and route; then validate current remit, contribution, corporate payer and participation directly.

Policy history and board-selection fit

Policy / governance discussion: Own AI-regulation preparation article establishes governance commentary, not formal regulator input.

June 21, 2010 - The Grill: Patricia Titus - Computerworld. Calls for clearer definitions of cyberwar and describes public-private input into government strategy. [Source: www.computerworld.com](http://www.computerworld.com)

Historical Unisys role and dated policy position; current field-CISO role is separate.

Benchmark: ISA recommendations, current ISA board practitioner profile, operating authority, company capacity, attributable policy work, concrete contribution, and portfolio balance. Corporate directorship alone does not determine priority.

Qualification status and ownership

Requirement	Evidence and remaining confirmation
Current role	Public role support; recheck directly before contact; direct confirmation pending.
ISA membership	Unknown current company/account and designated-representative status. Public board absence does not establish nonmembership.
Eligibility	Conditional representative fit. ISA acceptance and employer designation pending.
Board feedback / introducer	No named introducer established. Introduction completion: not confirmed.
Corporate sponsorship	Published annual dues \$75,000; corporate payer, budget approver and written authorization not confirmed.
Executive interest	Not directly confirmed. Published interest in cyber topics is not membership interest.
Time / participation	Four meetings yearly, including two in Washington, DC and two virtual, plus agreed preparation. Availability, travel and term commitment not confirmed.
ISA output and benefits	Person-specific hypotheses documented; prospect and employer acceptance not confirmed.
Portfolio	Industry/expertise rationale assessed. Work base and DC access require direct confirmation.

[ISA public board / meeting baseline](#) | [Bylaws](#) | [Published sponsorship](#)

1631 owns researched case and source accuracy; ISA owns current membership/eligibility/introducer decision; employer/prospect must confirm funding, interest, availability and proposed output.

Image and contact provenance

Portrait: Name-matched image on named public biography. Cropped from authentic named portrait to focus on face and shoulders. [Source: abnormal.ai](#)

Company mark: Current employer website brand asset [Source: abnormal.ai](#)

Attributable commentary and evidence ledger

10 / 10 substantive sightings recorded. Depth target met.

1. Preparing for AI Regulation: What CISOs Can Do Now | Abnormal AI

April 8, 2026 | Authored company article [Source: abnormal.ai](#)

Urges an enterprise AI inventory, accountable owners and human decisions about acceptable impacts rather than leaving AI governance entirely with security.

Attribution / limitation: Governance recommendations are the relevant evidence; this brief does not adopt the article's legal characterizations as legal advice.

2. Building a Culture of Proactive Threat Defense | Abnormal AI

March 11, 2026 | Authored article republished by employer [Source: abnormal.ai](#)

Advocates business context, collaboration and curiosity; humans interpret AI signals, while threat models and adaptive playbooks must evolve with operations.

Attribution / limitation: Republished from GRC Outlook; count the original and republication as one item.

3. If Every User Needs an Identity, Why Don't Our APIs? | Abnormal AI

February 5, 2026 | Authored company article [Source: abnormal.ai](#)

Says APIs need named owners, documented purpose and credential lifecycles, including narrow temporary privileges and automatic revocation.

Attribution / limitation: Public position; confirm current relevance and company sponsorship interest.

4. Building Stronger Cyber Defenses With AI - BankInfoSecurity

2025 | Direct video interview and publisher summary [Source: www.bankinfosecurity.com](#)

Discusses AI-enabled phishing and the need for behavioral defense against convincing impersonation.

Attribution / limitation: Interview summary is not a complete transcript or independent validation of a vendor's detection claims.

5. Federal Tech Podcast: for innovators, entrepreneurs, and CEOs who want to increase reach and improve brand awareness: Ep. 315 Behavioral AI Stops Advanced Federal Phishing Attacks

April 16, 2026 | Federal Tech Podcast interview summary [Source: sites.libsyn.com](#)

Explains learning normal communication behavior to identify anomalies in advanced phishing against federal users.

Attribution / limitation: Vendor-associated discussion; no independent efficacy finding and no ISA endorsement.

6. The Governance Model That Wasn't Built for This

2026-08-07 | Employer article with attributed remarks [Source: abnormal.ai](#)

Titus discusses the gap between human-centric identity governance and autonomous agents and service accounts.

Attribution / limitation: Other participants' views remain separately attributed; commercial employer publication.

ISA relevance: Potential ISA contribution inferred from documented governance, workforce or policy views; ISA interest and sponsorship unconfirmed.

7. When the Attack Looks Like the User

2026-08-10 | Employer article with attributed remarks [Source: abnormal.ai](#)

Titus distinguishes granting access from governing trust and discusses legitimate credentials used for illegitimate actions.

Attribution / limitation: Her incident examples are interview accounts, not independently verified incidents.

ISA relevance: Potential ISA contribution inferred from documented governance, workforce or policy views; ISA interest and sponsorship unconfirmed.

8. From Rules to Evidence

2026-08-11 | Coauthored employer article with named remarks [Source: abnormal.ai](#)

Titus argues that permissions need ongoing evidence of appropriate access rather than reliance on static grants.

Attribution / limitation: Coauthors Mike Britton and Piotr Wojtyla have separately attributed views.

ISA relevance: Potential ISA contribution inferred from documented governance, workforce or policy views; ISA interest and sponsorship unconfirmed.

9. The Attack Surface You've Already Built

2026-07-28 | Coauthored employer article [Source: abnormal.ai](#)

The joint article examines shadow AI, OAuth grants and abandoned permissions as sources of exposure.

Attribution / limitation: Titus is credited as a coauthor with Stephen Harrison and Mick Leach. This is a joint written position; their individual quotations are not assigned to her.

ISA relevance: Potential ISA contribution inferred from documented governance, workforce or policy views; ISA interest and sponsorship unconfirmed.

10. The Grill: Patricia Titus

2010-06-21 | Publisher executive Q&A [Source: www.computerworld.com](#)

Titus calls for clear cyberwar criteria and discusses public-private input into government cybersecurity strategy.

Attribution / limitation: Historical Unisys role and 2010 policy views; not present policy or proof of influence on adopted rules.

ISA relevance: Potential ISA contribution inferred from documented governance, workforce or policy views; ISA interest and sponsorship unconfirmed.

Prior ISA webinar engagement - supplied roster

Matched in ISA Webinar Attendees.xlsx, attendees.csv, row 332. Exact LinkedIn URL and supplied name/title reviewed; categorized FINAL v3 and v5 corroborate the row.

Supplied title: Global Cybersecurity Executive | Field CISO

Supplied organization: Abnormal AI. Registration does not establish current ISA membership, sponsorship interest or event attendance.

Individual webinar dates, repeat registrations, attendance and questions are not included in this source. Not counted toward ten substantive sightings.

Video titles and context for further review

Discovery leads below are not counted. Titles help prioritize review; the executive's actual remarks determine substance.

Season 2, Ep. 1 From Battlefield to Boardroom: Lessons in Cyber ... Source: www.youtube.com

Review context: Career and boardroom experience; screen for governance examples.

Attribution / duplicate check: Career story alone is not sustained policy activity; review exact remarks.