NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

01 JUL 2026

Foreign Adversary Influence in North Dakota

Report completed by the North Dakota State and Local intelligence Center, on behalf of the North Dakota Department of Emergency Services in fulfillment of the legislative requirements set forth in House Bill No. 1209 in the Sixty-ninth Legislative Assembly.

(U) This information may be protected under state law (N.D.C.C. Sections 44-04-18.1, 44-04-18.4(7), 44-04-18.7, 44-04-19.1, 44-04-24, 44-04-25, and 44-04-26) or applicable federal laws and may be withheld. Dissemination of Sensitive But Unclassified (SBU) information such as FOUO, CUI, DSEN, SSI, FISA, NOFORN, and LES information to the general public or media is not authorized. Disclosure of SBU information could jeopardize ongoing investigations and the safety of law enforcement personnel. Any relevant U.S. person information retained by the NDSLIC is in strict adherence to 28 CFR Part 23. In accordance with the fair use doctrine as codified by section 107 of the Federal Copyright Act of 1976, this is not an infringement of copyright; however, sources are cited at the end of each report for proper attribution.

(U) Table of Contents

(U) Introduction 4

Purpose, Scope and Methodology 5

Summary of Key Partners and Stakeholders Meeting 6

Survey Summary 7

Executive Summary 10

Overview of Findings 11

(U) Sector Analyses 12

HSA Prioritization 12

Energy 13

Electrical Subsector 18

Oil and Gas Subsector 22

Information Technology 27

Water & Wastewater 35

Healthcare and Public Health 42

Food and Agriculture 49

Emergency Services 57

Financial Services 62

Chemical 67

Communications 73

Transportation 80

Government Services and Facilities 87

Academia Subsector 93

Commercial Facilities 101

Dams 105

Critical Manufacturing 108

Nuclear Reactor, Materials, and Waste 112

Defense Industrial Base 116

(U) Evaluation of Existing Laws and Identification of Compliance Gaps 122

(U) Protection, Prevention, and Mitigation Recommendations 130

Overarching Strategies 130

Options for Consideration 132

(U) Conclusion 135

Summary of Findings and Call to Action 135

(U) Appendix A – Written Report to Legislative Management 138

Overview of Findings 138

Key Findings 138

Existing Authorities and Protections 139

What this Report Did Not Find 139

Identified Gaps 139

Private Sector Primacy 139

Fiscal Considerations 140

Overall Report Assessment 140

(U) Appendix B – Proposal for State Intelligence Unit 142

Background – Current Operation 142

Proposed Structure Change Recommendations 144

(U) Appendix C – Expressions of Likelihood (or Probability) 146

(U) Appendix D – Confidence and Threat in Sources Supporting Assessments and Judgments 147

Sources 148

(U) Appendix A: Written Report to Legislative Management

(U) Overview of Findings

Pursuant to House Bill 1209, the Department of Emergency Services conducted a comprehensive report of foreign adversary threats to North Dakota's critical infrastructure, economy, technology sectors, agricultural assets, and academic institutions. The report found that foreign adversaries particularly the People's Republic of China, Russian Federation, Islamic Republic of Iran, and Democratic People's Republic of Korea continue to present credible threats to the United States and North Dakota through cyber operations, economic influence, espionage, strategic investments, research exploitation, supply chain manipulation, and influence activities.

(U) This report found limited evidence that direct foreign ownership of North Dakota land currently represents a significant vulnerability in North Dakota. Rather, cybersecurity weaknesses, supply chain dependencies, foreign influence activities, security concerns, critical technology transfer, and interconnected infrastructure dependencies present greater overall risk. While foreign ownership of agricultural land remains a legitimate concern, available data indicates existing federal and state regulatory frameworks already provide significant oversight and mitigation mechanisms.

(U) Key Findings

The most significant cross-sector threat to North Dakota's critical infrastructure is cybersecurity. Foreign adversaries and cybercriminal actors are increasingly capable of exploiting interconnected information technology, operational technology, industrial control systems, cloud services, supply chains, and third-party service providers. These risks affect nearly every sector analyzed in this report and present the highest potential for cascading impacts.

Foreign land ownership remains an important issue but was not identified as the highest-risk threat vector when compared to cyber intrusion, supply chain dependency, research exploitation, foreign influence activity, and critical infrastructure interdependencies. Existing federal and state authorities provide partial mitigation; however, gaps remain in visibility, reporting, and coordination.

(U) North Dakota's critical infrastructure is highly interconnected. Disruptions affecting energy, communications, transportation, water, government services, agriculture, or information technology can rapidly cascade across multiple sectors. As a result, resilience planning, redundancy, continuity of operations, and public-private coordination are essential to reducing systemic risk.

(U) Foreign adversaries are increasingly using indirect methods to gain influence, collect intelligence, and exploit vulnerabilities. These include strategic investments, research partnerships, cyber-enabled espionage, talent recruitment programs, supply chain manipulation, misinformation and disinformation campaigns, and attempts to erode public trust in government institutions. North Dakota's ability to mitigate these risks depends on sustained information sharing, analytic capacity, cybersecurity support, suspicious activity reporting, and trusted partnerships among local, state, tribal, federal, academic, and private-sector stakeholders.

(U) Existing Authorities and Protections

(U) This report found that numerous federal authorities already exist to address foreign influence and national security concerns. These include the Committee on Foreign Investment in the United States (CFIUS), Foreign Investment Risk Review Modernization Act (FIRRMA), Agricultural Foreign Investment Disclosure Act (AFIDA), International Traffic in

Arms Regulations (ITAR), Export Administration Regulations (EAR), National Security Presidential Memorandum-33 (NSPM-33), federal banking regulations, sanctions authorities, and numerous sector-specific cybersecurity and security requirements.

(U) North Dakota likewise maintains several authorities that contribute to risk mitigation, including agricultural land ownership restrictions under North Dakota Century Code Chapter 47-10.1, intelligence sharing through the North Dakota State and Local Intelligence Center (NDSLIC), cybersecurity initiatives administered through North Dakota Information Technology (NDIT), and infrastructure protection activities conducted through the Department of Emergency Services. Collectively, these authorities provide substantial safeguards against foreign influence, espionage, cyber threats, and unauthorized technology transfer.

(U) What This Report Did Not Find

(U) This report did not identify direct foreign ownership of North Dakota land as a significant current foreign adversary threat to the state. While foreign land ownership remains a valid policy and national security concern, available information did not indicate that land ownership alone represents the highest-risk pathway for foreign adversary influence or disruption.

(U) This report also did not find that existing state business registration records are sufficient to determine whether an entity has a direct or indirect nexus to a foreign adversary nation. The Secretary of State's designation of an entity as "foreign" generally refers to an out-of-state entity, not necessarily a foreign nation-state connection. Additionally, the report did not identify a single sector-specific vulnerability that can be addressed through one policy solution. Instead, the threat environment is cross-sector, complex, and increasingly driven by cyber risk, supply chain dependencies, technology transfer, research security, foreign influence activity, and infrastructure interdependencies.

(U) Identified Gaps

(U) Despite existing protections, several challenges remain. Many foreign influence activities occur through indirect means such as research partnerships, cyber-enabled espionage, strategic investments, influence campaigns, shell companies, talent recruitment programs, and supply chain dependencies. Existing authorities are often better suited to addressing ownership and transactions than influence and access.

(U) Stakeholder engagement also identified challenges related to information sharing, situational awareness, reporting mechanisms, and state visibility into certain federal review processes. Confidentiality requirements surrounding CFIUS proceedings limit state awareness of foreign investment reviews affecting North Dakota. Additionally, many critical infrastructure sectors remain privately owned and operated, limiting the state's authority to mandate security measures.

(U) Private Sector Primacy

A significant portion of North Dakota's critical infrastructure is privately owned and operated. As a result, private-sector owners and operators retain primary responsibility for securing their facilities, networks, systems, personnel, data, and supply chains. The state's role is generally not to assume operational control of private infrastructure, but to support risk reduction through coordination, information sharing, technical assistance, training, outreach, threat awareness, emergency management support, and facilitation of federal resources.

(U) North Dakota's most effective role is therefore one of enabling, coordinating, and supporting resilience across sectors. State agencies can help identify emerging risks, share threat information, coordinate preparedness activities,

support suspicious activity reporting, facilitate cybersecurity resources, and connect infrastructure owners with federal partners such as CISA, FBI, USDA, DOE, DCSA, and other sector-specific agencies.

(U) Legislative Options for Consideration

(U) Based upon stakeholder input, survey results, and threat analysis, the Legislature may wish to consider several policy options:

- Development of a Select Committee on Intelligence designed to ensure key state leaders such as legislative leadership, Governor, Attorney General, Secretary of State, and Agricultural Commissioner are able to be briefed on sensitive and/or classified materials so that state policy can be crafted and implemented in a manner consistent with the actual or projected threat environment. In addition, the committee shall monitor, review, and supervise the activities of the state intelligence unit to ensure compliance with the Constitution, state, and federal laws, and executive orders.
- To facilitate trusted information sharing, consider formally adopting and adhering to the federal SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU) framework. Applying consistent administrative controls for sensitive information that does not meet classification thresholds will enhance the state's ability to exchange intelligence with federal partners, local governments, law enforcement, and private-sector stakeholders who have a legitimate right and need to know, while protecting sensitive data from inappropriate disclosure.
- Codifying the North Dakota State and Local Intelligence Center (NDSLIC) in North Dakota Century Code to provide long-term organizational stability, clarify authorities, and establish sustainable state funding.
- Expanding intelligence, cybersecurity, and critical infrastructure analytic capabilities through additional full-time staff positions.
- Expanding intelligence analytic capabilities through investment in closed artificial intelligence systems to identify foreign adversarial threats and risk assessment tools.
- Enhancing suspicious activity reporting (SAR) education, outreach, and reporting mechanisms for public and private sector stakeholders.
- Establishing secure information-sharing technologies and CJIS-compliant communications platforms to support intelligence and threat reporting.
- Increasing outreach concerning foreign influence, research security, cybersecurity, and agricultural investment reporting requirements.
- Evaluating mechanisms for reviewing designated high-risk transactions involving foreign adversaries while ensuring due process protections and maintaining a favorable business climate. In addition, a formal divesture process and structure should be codified when high risk transactions occur.
- Supporting continued public-private partnerships, cybersecurity investments, critical infrastructure assessments, and resilience initiatives across all sectors.

(U) Fiscal Considerations

(U) Most recommendations identified within this report can be implemented incrementally through a combination of existing state resources, federal grant funding, and targeted legislative appropriations. However, recommendations involving additional personnel, technology platforms, intelligence capabilities, analytic tools, and infrastructure protection programs would require further fiscal analysis and appropriation decisions by the Legislative Assembly.

(U) Sustained state funding would reduce reliance on federal grant cycles and allow North Dakota to prioritize state-specific threats, vulnerabilities, and policy objectives. Federal grant funding, including the Homeland Security Grant

Program, should continue to supplement state efforts where appropriate, but core capabilities such as intelligence analysis, critical infrastructure protection, cybersecurity coordination, and information sharing may benefit from more predictable state support.

(U) Overall Report Assessment

(U) This report concludes that North Dakota faces an evolving foreign adversary threat environment that is increasingly characterized by cyber operations, technological competition, economic influence, supply chain vulnerabilities, research exploitation, and strategic information activities rather than traditional land acquisition alone. Consequently, the most effective long-term strategy for reducing risk is likely to focus on strengthening cybersecurity, enhancing intelligence and information sharing, improving infrastructure resilience, increasing public-private collaboration, and maintaining awareness of emerging foreign influence activities while preserving North Dakota's economic competitiveness and business-friendly environment.

(U) North Dakota's policy response should be practical, evidence-based, and scalable. Future actions should avoid unnecessary burdens on legitimate commerce, agriculture, academia, and investment while ensuring that the state has the capability to identify, assess, report, and respond to credible foreign adversary risks. A balanced approach that combines state-level capacity, federal coordination, public-private partnerships, and targeted legislative action will best position North Dakota to protect its critical infrastructure, economy, and citizens.

(U) Appendix B: Proposal for State Intelligence Unit

(U) Background – Current Operations

(U) The NDSLIC, re-authorized by Governor Jack Dalrymple on March 25, 2014, in Executive Order 2014-06, is set up to help the efforts of the United States government to establish a national network of Fusion Centers, which will serve as the "central hub" of North Dakota's fusion process and serve as the primary interface between North Dakota and the Federal Government for information gathering, analysis and dissemination. The NDSLIC Executive Board, set by Executive Order 2007-06, is comprised of the Adjutant General of the North Dakota National Guard, the Director of the North Dakota Bureau of Criminal Investigation, the Colonel of the North Dakota Highway Patrol, Director of the North Dakota Division of Homeland Security, and the North Dakota Information Technology Department Chief Information Officer. The NDSLIC Executive Board has the primary responsibility for the overall operation of the NDSLIC including, but not limited to, its information systems, personnel, and operations.

- **(U) Mission**
  - The mission of the North Dakota State & Local Intelligence Center (NDSLIC) is to gather, store, analyze and disseminate information on crimes, both real and suspected, to the law enforcement community, government officials and private industry concerning dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purposes of decision making, public safety and proactive law enforcement while ensuring the rights and privacy of citizens.
- **(U) Function**
  - (U) The North Dakota State and Local Intelligence Center (NDSLIC) is the central point for inter/intra agency information sharing. It is responsible for the review, analysis, and dissemination of pertinent homeland security and law enforcement intelligence. As the state fusion center, the NDSLIC is the liaison between federal, state, local and tribal agencies helping to combat major criminal threats and improve counter-terrorism strategies. The NDSLIC provides essential intelligence and operational coordination to private and public industry representatives and law enforcement (local, state, federal, and tribal) to ensure safety and security across all sectors. The NDSLIC is responsible for providing the North Dakota Homeland Security Advisor and the Governor's Office with timely information as it relates to acts of terrorism or terrorist threats that directly impact North Dakota or our nation.
- **(U) Personnel**
  - NDSLIC Director (NDBCI – SSA Agent)
    - Provides overall leadership and operational control of the NDSLIC. Directly supervises NDBCI analyst staff and serves as primary liaison to the Executive Board, Governor's Office, and federal partners.
      - Oversee day-to-day operations, personnel, and intelligence functions in accordance with state and federal law.
      - Report to the Executive Board and Governor's Office as required.
      - Ensure NDSLIC operations comply with privacy, civil rights, and civil liberties protections.
      - Approve and review NDSLIC policies, SOPs, and analytic products.
      - Maintain strong communication with federal partners, state agencies, local law enforcement, and the private sector.
      - Ensure the Center fulfills its strategic priorities:
      - Provide timely, actionable intelligence to stakeholders.
      - Support SAR, TTL, and critical incident reporting.

- Oversee outreach and stakeholder engagement.
- Support cyber and CIKR protection capabilities.
- Ensure staff training and professional development.
- Oversee fiscal responsibility for budgets, grants, and resource allocation.
- Maintain continuity of operations (COOP) and designate leadership during emergencies.

- NDSLIC Deputy Director / Privacy Officer (NDDES Protection Section Chief)
  - Serves as second-in-command and Acting Director when required. Provides daily operational, administrative, and training oversight. Supervises the CIKR Program Manager and coordinates with the Senior Threat Analyst and NDITD Cyber Analysts. Serves as designated Privacy Officer.
    - Support the Director in overseeing daily operations, personnel, and intelligence functions.
    - Act as Acting Director when required.
    - Serve as Privacy Officer: ensure compliance with NDSLIC Privacy Policy, oversee CRCL training, and review policies/products for compliance.
    - Review NDSLIC policies, SOPs, and analytic products as delegated.
    - Maintain communication with federal, state, and local partners.
    - Ensure program areas fulfill strategic priorities including intelligence delivery, TTL reporting, outreach, cyber/CIKR, and training.
    - Supervise the CIKR and Outreach Program and coordinate with the Senior Threat Analyst and Cyber Analysts.
    - Serve as Homeland Security Advisor's designee for state/local clearances.
    - Serve as Security Manager for NDSLIC and NDDES.
- Critical Infrastructure Outreach and Program Manager (NDDES)
  - Leads the statewide Critical Infrastructure Program and Outreach, including the Information Liaison Officer (ILO) program. Reports to the Deputy Director.
    - Supervise the Critical Infrastructure Analyst (this position is currently vacant).
    - Manage the Critical Infrastructure ILO program.
    - Conduct Site Assessment Visits (SAVs) and produce reports.
    - Serve as point of contact for DHS data calls and special event reporting.
    - Produce the monthly CIKR Ticker.
    - Fulfilling RFIs related to infrastructure and outreach.
    - Maintain outreach with public and private sector partners.
- NDITD Cyber Analysts
  - Serve as coordination staff supporting statewide cyber intelligence and incident response.
    - Collect and analyze cyber threat reporting.
    - Produce and review cyber products.
    - Provide technical and investigative support.
    - Respond to incidents and assist with cyber investigations.
    - Contribute to North Dakota's Cyber Response Strategy.
- NDSLIC Criminal Intelligence Analysts (NDBCI)
  - Provide analytic and operational support for criminal intelligence. Report to the Director for personnel; tasking coordinated with the Deputy Director.

- Collect and compile intelligence from multiple sources.
- Develop investigative leads, timelines, flow charts, and trend analyses.
- Produce analytic products, assessments, and situational reports.
- Support law enforcement cases and prosecutions.
- Provide training and briefings on intelligence trends.
- Maintain accuracy and integrity of intelligence databases.
- Produce recurring outputs: RFIs, Weekly Overviews, Hot Sheets, BOLOs.

  - NDHP Liaison / Law Enforcement ILO (NDHP Sergeant)
    - Supports statewide law enforcement information sharing through the ILO program. Provides outreach, training, and incident coordination on behalf of the NDSLIC.
      - Recruit, train, and coordinate ILOs across North Dakota.
      -
      - Serve as the primary point of contact between the statewide ILO network and the NDSLIC.
      - Deliver and assist in specialized training programs, including active shooter preparedness and response.
      - Teach and present at law enforcement and intelligence-related training events.
      - Represent the NDSLIC at intelligence and public safety meetings across the state.
      - Assist the Critical Infrastructure/Outreach Program Manager with Site Assessment Visits (SAVs) and reporting.
      - Conduct outreach with local law enforcement agencies to strengthen information-sharing partnerships.
      - Support incident information flow by coordinating with ILOs and relaying field-level observations to the NDSLIC.

- **(U) Procedures**
  - The North Dakota State and Local Intelligence Center (NDSLIC) maintains a comprehensive list of Standard Operating Procedures (SOPs) that govern personnel management, operational activities, intelligence processes, and strategic functions. These procedures are designed to ensure compliance with applicable federal and state laws, regulations, policies, privacy and civil liberties protections while supporting the Center's mission and operational objectives. These SOPs have been determined to be “Confidential Records” by the State of North Dakota.
- **(U) Budget**
  - The NDSLIC is heavily reliant on funding provided through the Homeland Security Grant Program (HSGP) to sustain core operational capabilities. Five of the Center's twelve full-time positions including the Director, Deputy Director, Critical Infrastructure Program Manager, Law Enforcement Intelligence Liaison Officer (ILO), and Cyber Analyst are fully or partially funded through HSGP resources. The remaining personnel are funded by their respective parent agencies. Operational expenses not covered by HSGP are absorbed through participating agencies' general fund budgets.

(U) Proposed Structure Change Recommendations

(U) Rescind Executive Order 2014-06 and formally establish the North Dakota State and Local Intelligence Center (NDSLIC) in North Dakota Century Code. Codifying the NDSLIC in state law would provide long-term organizational stability, clarify authorities and responsibilities, and ensure continuity of operations regardless of future administrative changes.

(U) As part of this transition, the Legislature should establish a dedicated appropriation to support personnel, administrative, technology, training, and operational expenses necessary to sustain the Center's core mission. Federal grant funding, including the Homeland Security Grant Program (HSGP), would continue to supplement operations (if it is available) and be administered through the North Dakota Department of Emergency Services (NDDES) consistent with current practices.

(U) The NDSLIC would remain a collaborative, multi-agency intelligence and information-sharing organization comprised of local, state, tribal, federal, and private-sector partners. Existing staff assignments, governance structures, mission responsibilities, and interagency partnerships would remain unchanged unless modified through future policy decisions. Current plans, policies, procedures, privacy protections, and civil liberties safeguards would remain in effect and continue to be reviewed and updated as necessary to ensure compliance with applicable state and federal laws, regulations, and intelligence best practices.

(U) Appendix C: Expressions of Likelihood (or Probability)

(U) Phrases such as "the NDSLIC judges" and "the NDSLIC assesses" and terms such as "likely" and "probably" convey analytical judgments and assessments. The chart approximates how expressions of likelihood and probability correlate with percentages of chance.

UNCLASSIFIED[dlviii]

Terms of Likelihood	Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain(ly)
Terms of Probability	Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
	1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

(U) Unless otherwise stated, the NDSLIC does not derive judgments via statistical analysis.

(U) Appendix D: Confidence and Threat in Sources Supporting Assessments and Judgments

(U) Confidence levels reflect the quality and quantity of the source information supporting judgment. Consequently, the NDSLIC ascribes high, medium, or low levels of confidence to assessments, as follows:

(U) **High confidence** generally indicates the NDSLIC's judgments are based on high quality information, from multiple sources. High confidence in a judgment does not imply the assessment is a fact or a certainty; such judgments might be wrong. While additional reporting and information sources may change analytical judgments, such changes are most likely to be refinements and not substantial in nature.

(U) **Medium confidence** generally means the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. Additional reporting or information sources have the potential to increase the NDSLIC's confidence levels or substantively change analytical judgments.

(U) **Low confidence** generally means the information's credibility or plausibility is uncertain, the information is too fragmented or poorly corroborated to make solid analytic inferences, or the reliability of the sources is questionable. Absent additional reporting or information sources, analytical judgments should be considered preliminary in nature.

(U) **High threat indicates** that there is evidence to suggest or indicate that individuals have expressed intent, capability, and opportunity to carry out a particular act, whether it is a terror attack, fundraising, radicalization, or criminal activity, or the activity is ongoing and significant in volume.

(U) **Medium threat** indicates there is evidence to suggest that individuals have two of the three components necessary to commit an act or the activity is ongoing but limited in volume.

(U) **Low threat** indicate that existing evidence suggests an individual possesses one of none of the components necessary to commit an act or the activity is sporadic or non-existent.

(U) Sources

[dlviii] (U) Office of the Director of National Intelligence; Intelligence Community Directive 203 Technical Amendment – Analytic Standards; https://www.dni.gov/files/documents/ICD/ICD-203.pdf; 12 June 2023; 11 SEPT 2025; UNCLASSIFIED// UNCLASSIFIED; UNCLASSIFIED// UNCLASSIFIED; Source is a federal government agency.