

**OFFICE of
PRIVATE SECTOR****Liaison Information Report (LIR)****CROSS-SECTOR****28 AUGUST 2024****LIR 240828008****Cuban Intelligence Services Use Recruited Professors
and Academics to Target Students**

References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI. The FBI does not and will not target people based on their race or ethnicity. Potential criminality exhibited by certain members of groups referenced herein does not negate nor is it a comment on the constitutional rights of the group itself or its members to exercise their rights under the First Amendment to the U.S. Constitution. The FBI does not investigate, collect, or maintain information on any U.S. person solely for the purpose of monitoring activities protected by the First Amendment.

The FBI's Counterintelligence Division and Boston Field Office, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform U.S. academic institutions on strategies and tradecraft of the Cuban Intelligence Services (CuIS) to target students using recruited academic personnel to spot^a and assess potential recruits. This report should be read in conjunction with LIR 230211010 released on 11 December 2023 titled, "Recruitment Efforts of Cuba's Intelligence Services in Academia," which provided case examples of experts and government personnel who collected and passed classified or sensitive information.

Cuban intelligence views U.S. universities as high priority targets in their efforts to fulfill the strategic objectives and goals of the Cuban government, as sources of foreign policy expertise, future government leadership, and as broadly informing U.S. public opinion. The CuIS has sought to recruit professors and academic leadership to spot, assess, and recruit students who may have future access to sensitive or classified information, or who may enter a position of foreign policy development and influence.

The CuIS invests in long term recruitment operations at U.S. academic institutions. In one exemplary case, the CuIS recruited and operated a network of professors and researchers at two prominent U.S. universities over the course of 30 years, from the 1970s through the 2000s, and exploited the professors' standing within the academic community and their placement as mentors and advisors to assess and recruit students.

- The CuIS network's principal agent^b, a now deceased U.S. professor, claimed to have assessed as many as 50 students and colleagues, and recruited at least six motivated by admiration and loyalty; one of the recruits claimed that proving their worth to the professor, who had been a mentor and doctoral dissertation committee member, was their primary motivation.

^a Spotting is identifying an individual with access to desired information and assessing is identifying the individual's vulnerabilities and determining whether they may be susceptible to recruitment.

^b In a principal agent network, a group of recruited assets is handled by a leading asset or agent who serves as the network's liaison to an intelligence service.

**OFFICE of
PRIVATE SECTOR****Liaison Information Report (LIR)**

- The U.S. professor principal agent claimed to have assessed and groomed students for recruitment by determining their willingness to engage in open, unclassified research, determining their political leanings, and then guiding them to engage in more discrete work. The U.S. professor then induced them to meet secretly with Cuban intelligence.
- The CuIS tasked this academic network with spotting and assessing their students and colleagues to identify possible recruits. The CuIS provided guidance on preferred personality types, suitability, age, race, nationality, and professional access.
- The network communicated among themselves and with the CuIS using clandestine communications methods such as email addresses established for covert communications; shortwave radio transmissions; instructions on concealed water-soluble paper; and verbal paroles.^c Members of the network agreed to provide CuIS with biological research, guidance on Cuba's biological defense program, and biological reagents. Critically, the CuIS shared the network's information with other foreign governments, including the Democratic People's Republic of Korea and the Russian intelligence services.

The CuIS also exploit domestic and international exchanges for academic recruitment operations. Cuban intelligence – sometimes embedded in delegations - uses information on visiting students and researchers, including that obtained from other recruited university personnel, to design targeted recruitment operations and approaches.

An indicator alone does not determine targeting or recruitment activity; academic institutions should evaluate the totality of the potential recruitment behavior, including communications and other relevant circumstances before notifying security/law enforcement personnel.

The following suspicious activities/indicators include, but are not limited to any individual, group, or business; observe these indicators in context:

- Requests to clandestinely engage in research or other work outside of the student's or academic's normal area of inquiry;
- Requests to communicate via non-official, personal, or secret accounts, apps, or other means, or in channels inaccessible to the student's or researcher's institution;
- Inducements to engage in undisclosed meetings with foreign government officials;
- Requests to access, obtain, or provide information that may be proprietary, sensitive, export-controlled, classified, or personally identifiable (PII) outside of the student's or academic's normal area of inquiry, and/or without the express authorization of the student's or academic's institution^d; or

^c Verbal paroles are a sequence of statements meant to authenticate identities.

^d The CuIS has been known to recruit individuals based on potential future access to classified or sensitive information. Individuals without current access may still be assessed for future recruitment.



OFFICE of PRIVATE SECTOR





Liaison Information Report (LIR)

- Requests from foreign government representatives to attend meetings, conferences, or social events and report on other attendees and participants.

Researchers may be sensitized to these issues through instruction on appropriate handling of PII, intellectual property, classified, sensitive, or export-controlled information; policies regarding administration, faculty, and student interactions with foreign government officials; and guidance on the proper channels to report activity of concern. Institutions may be encouraged to provide training to increase awareness of policies regarding foreign intelligence threats and capabilities while traveling overseas or while hosting foreign delegations to U.S. institutions.

The FBI’s Office of Private Sector disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.

Traffic Light Protocol (TLP) Definition

Color	When should it be used?	How may it be shared?
<p>TLP: RED</p>  <p>For the eyes and ears of individual recipients only, no further disclosure.</p>	<p>Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.</p>	<p>Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.</p>
<p>TLP: AMBER</p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP: AMBER+STRICT restricts sharing to the organization only.</p>	<p>Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP: AMBER+STRICT.</p>
<p>TLP: GREEN</p>  <p>Limited disclosure, recipients can spread this within their community.</p>	<p>Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.</p>
<p>TLP: CLEAR</p>  <p>Recipients can spread this to the world, there is no limit on disclosure.</p>	<p>Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.</p>