

# FBI IMAGINES USING ASSESSMENTS TO RECRUIT US ENGINEERS FOR INSIGHT ONTO SPYING IN SEMICONDUCTOR INDUSTRY

For something else, I'm reviewing the section of the FBI Domestic Investigations and Operations Guide on assessments made available in unredacted form to the Intercept. Of particular interest are the scenarios the DIOG uses to explain whether an Agent would or could use an assessment to collect information without opening a preliminary investigation. One way the FBI uses assessments is to identify potential informants. As one of the scenarios for when it might do so, it uses the example of trying to find out about a particular country X's targeting of engineers and high tech workers involved in the production of semiconductor chips. For an engineer who travels frequently to country X, the FBI might either target him, or try to recruit him. (see page 117)

(U//FOUO) *Example B:* A field office has a Full Investigation open on a group of individuals from country X believed to be targeting engineers and high-tech workers involved in the production of semiconductor chips. Evidence in the Full Investigation suggests that the individuals from country X are attempting to recruit the engineers and high tech workers to steal information regarding the semiconductor chips in exchange for money. During the investigation, an engineer who travels frequently to country X has been identified.

(U//FOUO) *Response B:* Information developed during the Predicated Investigation may be used to determine whether the engineer should be viewed as a subject of the investigation or a potential CHS. If the engineer is determined to be a subject of the Full Investigation, a Type 5 Assessment may not be opened and the engineer needs to be opened as the target of a Full Investigation. If the primary focus of the FBI's interest is to determine whether the individual may be a potential source, a Type 5 Assessment should be opened to collect information necessary to determine whether the FBI should attempt to recruit the engineer as a CHS.

This is important for two reasons. First, the FBI is permitted to search FBI's own databases to conduct this assessment. That would include information collected via Section 702. So when people talk about the risks of back door

searches, it could mean a completely innocent engineer getting targeted for recruitment as an informant.

The other reason this is important is because it is precisely what appears to have happened with Professor Xiaoxing Xi, who was falsely accused of sharing semiconductor technology with China. After Xi and his attorney Peter Zeidenberg explained to the FBI that they had badly misunderstood the technology they were looking at, the case against Xi was dismissed.

In fact, Xi claims in a lawsuit against the government that the emails on which was the case was built were improperly searched using Section 702 or EO 12333.

On information and belief, both before and after obtaining the FISA orders, defendant Haugen and/or Doe(s) caused the interception of Professor Xi's communications, including his emails, text messages, and/or phone calls, without obtaining a warrant from any court. In conducting this surveillance, the defendants may have relied on the purported authority of Section 702 of FISA or Executive Order 12333. Although neither Section 702 nor Executive Order 12333 permits the government to "target" Americans directly, the government nonetheless relies on these authorities to obtain without a warrant the communications of Americans who are in contact with individuals abroad, as Professor Xi was with his family and in the course of his scientific and academic work.

On information and belief, defendant Haugen and/or defendant Does searched law enforcement databases for communications of Professor Xi that the government had intercepted without a warrant, including his private communications intercepted under Section 702 of FISA and Executive Order 12333,

and examined, retained, and/or used such communications.

[snip]

The actions of defendants Haugen and/or Doe(s) in searching law enforcement databases for, examining, retaining, and using Professor Xi's communications, including his emails, text messages, and/or phone calls, that were obtained without a warrant, and without notice to Professor Xi, violated Professor Xi's clearly established constitutional rights against unlawful search and seizure and his right to privacy under the Fourth Amendment.

Given how closely this scenario matches his own case, I'd say the chances his emails were first identified via a back door search are quite high. Note, too, that Temple University, where he works, has its email provided by Google, meaning these emails might be available on via PRISM.

Of additional interest, the one description of sensitive potential Confidential Human Sources that the officially released DIOG redacts which is revealed in the Intercept copy is academic personnel. (see page 112)

(U//FOUO) A member of the faculty or the administration of a college or university in the United States.

So they *will* recruit professors like Professor Xi as informants – they would just require special approval to do so.