



Yuksel Senbol

- 36-year-old owner of US-based front company
- Conspired with two Turkish nationals who were already debarred from contracting with the US Government
- Facilitated Turkish nationals' effort to fraudulently supply critical military components to the United States
- Assisted Turkish nationals in obtaining sensitive export-controlled drawings
- Sentenced to 15 months and ordered to forfeit \$275,000



CDSE

Center for Development
of Security Excellence

CASE STUDY

Fraud

WHAT HAPPENED

Yuksel Senbol, 36, of Orlando, Florida, operated a fraudulent front company to facilitate the illegal export of sensitive U.S. military technology to Turkish co-conspirators, who in turn manufactured substandard defense componentry for resale back to the United States DOD.

Beginning in April 2019, Senbol established Mason Engineering Parts LLC as a front company to assist Turkish co-conspirators Mehmet Ozcan and Onur Simsek in fraudulently obtaining DOD contracts. The scheme involved representing Mason Engineering Parts as a vetted U.S. manufacturer when parts were in fact manufactured in Turkey.

To enable overseas manufacturing, Senbol facilitated the illegal export of export-controlled drawings of critical U.S. military technology. Using remote access software, she allowed Ozcan to control her computer from Turkey, bypassing security restrictions intended to limit access to sensitive military drawings to computers within the United States.

After manufacturing in Turkey, components were shipped to Senbol, who repackaged them and removed all references to their Turkish origin. The conspirators then lied about the parts' origin to receive payment from the U.S. Government and contractors. Senbol laundered hundreds of thousands of dollars in proceeds back to Turkey through international wire transfers, personally profiting from the scheme.

The scheme continued until uncovered by Federal investigators.

Senbol pleaded guilty on May 7, 2024, to 25 felony counts, including the conspiracy to defraud the United States, conspiracy to commit wire fraud, conspiracy to commit money laundering, seven counts of money laundering, conspiracy to violate the Export Control Reform Act (ECRA), four counts of violating the ECRA, and one count of violating the Arms Export Control Act.

On October 24, 2024, she was sentenced to 15 months in prison and ordered to forfeit \$275,430.90.

INDICATORS

Foreign Influence – Senbol maintained significant ties to Turkey, including through her co-conspirators.

Tradecraft – Senbol used remote access software that allowed Ozcan to “evade security restrictions that limited access to these sensitive military drawings to computers within the United States.”

Quality Control Failures – Parts supplied by Senbol failed military testing and did not conform to specifications.

IMPACT

- The components were intended for use in Navy Nimitz and Ford Class Aircraft Carriers, Navy Submarines, Marine Corps Armored Vehicles, and Army M-60 Series Tank and Abrahams Battle Tanks. According to investigators, many components were “critical application items,” meaning failure of these components would have potentially rendered the end systems inoperable.
- According to court documents, the “[p]arts supplied by Senbol were tested by the U.S. military and were determined not to conform with product specifications.” The substandard components posed significant risks to military readiness and personnel safety.

ADDITIONAL

- Senbol knew that co-conspirator Onur Simsek had been debarred from U.S. Government contracting after being convicted of a “virtually identical scheme” in the Southern District of Florida.
- The scheme involved systematic deception: Senbol repackaged Turkish-manufactured components, “making sure to remove any reference to their Turkish origin” before delivery to the U.S. Government and contractors.
- Co-conspirators Mehmet Ozcan and Onur Simsek remain fugitives from justice.

Questions to Consider:

- How does your organization verify the authenticity and qualifications of defense contractors claiming to be domestic manufacturers?
- What controls are in place to prevent unauthorized remote access to export-controlled technical data?

Resources for further exploration:

- Export Control Reform Act (ECRA) (<https://www.congress.gov/crs-product/R46814>)
- Arms Export Control Act (AECA) (<https://samm.dsca.mil/glossary/arms-export-control-act-aeca>)
- Foreign Ownership, Control, and Influence (FOCI) (<https://www.dcsa.mil/FOCI/>)

Supporting Through Reporting!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager