Two recent settlements for export control violations demonstrate both the value of voluntary self-disclosures and the potential costs.

By Ulrika Swanson

In April 2021, German software company SAP SE ("SAP") agreed to pay combined penalties of more than $8 million as part of a global resolution with the Departments of Justice, Commerce, and Treasury. As part of this resolution, DOJ's National Security Division ("NSD") and the U.S. Attorney's Office for the District of Massachusetts entered into a non-prosecution agreement with SAP, under which SAP will disgorge $5.14 million of ill-gotten gain. SAP entered into separate settlement agreements with OFAC and BIS, with the BIS settlement agreement requiring that SAP conduct internal audits of its compliance with U.S. export control laws and regulations for a period of three years.

This is the first application of DOJ's Export Control and Sanctions Enforcement Policy, which encourages companies to voluntarily self-disclose all potentially willful violations of the statutes implementing the U.S. government's primary export control and sanctions regimes. When a company (1) voluntarily self-discloses export control or sanctions violations to NSD's Counterintelligence and Export Control Section ("CES"), (2) fully cooperates, and (3) timely and appropriately remediates, there is a presumption that the company will receive a non-prosecution agreement and will not pay a fine, absent aggravating factors.

Here, SAP submitted voluntary self-disclosures to NSD, OFAC, and BIS, acknowledging violations of the Export Administration Regulations and the Iranian Transactions and Sanctions Regulations. Between 2010 and 2017, SAP's U.S.-headquartered Content Delivery Provider released SAP software, upgrades, and/or patches 5,787 times to SAP users in Iran, allowing those users to access and download SAP technology; SAP's own servers released an additional 19,567 downloads to Iran. These 25,354 downloads went to 14 Iranian shell companies and several multinational companies. SAP further failed to implement audit recommendations related to screening, institute processes to investigate whistleblower complaints, and conduct adequate due diligence.

SAP received full credit for its cooperation, which included conducting a thorough internal investigation, proactively identifying issues and facts that would likely be of interest, and providing regular updates to the agencies. Although avoiding the filing of criminal charges, and potential civil penalties as high as $56 million, SAP spent more than $27 million on remediation over the last four years, including: (1) implementing GeoIP blocking; (2) deactivating thousands of individual users of SAP cloud based services based in Iran; (3) transitioning to automated sanctioned party screening of its Cloud Business Group companies; (4) auditing and suspending SAP partners that sold to Iran-affiliated customers; (5) hiring of experienced U.S.-based export controls staff; and (6) conducting more robust due diligence at the acquisition stage by requiring new acquisitions to adopt GeoIP blocking and requiring involvement of the Export Control Team before acquisition.

Honeywell International, Inc. ("Honeywell") had similar results after submitting a voluntary self-disclosure to the State Department involving 34 violations of the Arms Export Control Act and

the International Traffic in Arms Regulations. These violations related to aerospace and defense technical data (engineering prints for castings and parts for aircraft, gas turbine engines, and military electronics) exported to recipients in Canada, Mexico, Ireland, China, and Taiwan without government approval. Honeywell and DDTC settled these allegations in a Consent Agreement that will remain in place for three years.

Honeywell potentially would have faced $37.4 million in civil penalties for the alleged violations. Instead, Honeywell's settlement requires that it pay $13 million, $5 million of which was assessed for remedial compliance measures. Additionally, Honeywell agreed to implement remedial measures that must remain in effect for the duration of the Consent Agreement, including the following:

- In consultation with and with the approval of the Director of the DDTC, Honeywell must designate a qualified official to serve as a Special Compliance Officer or Internal Special Compliance Officer, who will provide status reports to the CEO and DDTC concerning its compliance with the Consent Agreement and AECA and ITAR regulated activities;
- Honeywell must institute strengthened corporate compliance procedures, including training related to the AECA and ITAR for employees;
- Honeywell must implement a comprehensive automated export compliance system, and provide to DDTC an update outlining the status every six months;
- At minimum, one audit shall be performed during the term of the Consent Agreement, with a draft plan submitted to DDTC for review and approval, and a post-audit report submitted to DDTC to confirm whether Honeywell addressed the findings described in the written audit report; DDTC will then determine whether additional audits are required;
- Honeywell must arrange and facilitate, with minimum advance notice, on-site reviews by DDTC while the Consent Agreement remains in effect.

As these settlements demonstrate, voluntary self-disclosures are encouraged by the agencies, and can be a significant mitigating factor when it comes to penalties and potential criminal liabilities; however, the remediation costs can be substantial.