DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: April 29, 2021

OFAC Settles with SAP SE for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations

SAP SE ("SAP"), a software company headquartered in Walldorf, Germany that provides enterprise application software, cloud-based services, and associated maintenance and support, has agreed to pay $2,132,174 to settle its potential civil liability for 190 apparent violations involving the export of software and related services from the United States to Iran. These violations arose from SAP's exportation of software and related services from the United States to companies in third countries with knowledge or reason to know the software or services were intended specifically for Iran, as well as from the sale of cloud-based software subscription services accessed remotely through SAP's cloud businesses in the United States to customers that made the services available to their employees in Iran. The settlement amount reflects OFAC's determination that SAP's conduct was non-egregious and voluntarily self-disclosed, and accounts for SAP's remedial response.

SAP was concurrently investigated by the U.S. Department of Justice (DOJ) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS), resulting in a non-prosecution agreement with DOJ and a settlement agreement with BIS. SAP's obligation to pay the settlement amount due to OFAC shall be deemed satisfied by SAP's payment of a greater amount in satisfaction of penalties assessed by DOJ and BIS arising from the same course of conduct.

Description of the Conduct Leading to the Apparent Violations

From approximately June 1, 2013 to January 1, 2018, SAP authorized 13 sales of SAP software licenses, 169 sales of related maintenance services and updates, and eight sales of cloud-based subscription services. The sales of SAP software licenses and related maintenances services and updates (collectively "SAP software") were sold by third-party resellers ("SAP Partners") in Turkey, the United Arab Emirates (UAE), Germany, and Malaysia. SAP Partners in these countries sold these licenses and services to companies in third countries, including companies controlled by Iranian companies, that provided the SAP software to users in Iran. SAP referred to these third-country companies as "pass-through entities." The software was delivered from SAP servers in the United States and SAP's U.S.-headquartered content delivery provider. The sales of cloud-based subscription services to third country-based customers that then provided access to users located in Iran were conducted by two of SAP's cloud business group subsidiaries in the United States, with SAP's knowledge or reason to know the services would be provided specifically to Iran.

In doing so, SAP appears to have violated § 560.204 of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR), prohibiting the export, re-export, sale, or supply, directly or indirectly from the United States, or by a United States person, wherever located, of any goods, technology, or services to companies and individuals in Iran, including the export, re-export, sale, or supply to a third country undertaken with knowledge or reason to know the goods, technology, or

services are intended specifically for Iran (the "Apparent Violations"). The total value of the transactions constituting the Apparent Violations is $3,693,898.

Sales to "Pass-Through" Entities

The Apparent Violations connected with the sales of SAP software by SAP Partners to pass-through entities were caused in part by shortcomings in SAP's compliance processes. For example, internal audits conducted in 2006, 2007, 2010, and 2014 found that SAP did not screen customers' Internet Protocol (IP) addresses, resulting in SAP's inability to identify the country in which SAP software was downloaded. This deficiency, the audits found, put SAP at risk of breaching U.S. economic sanctions and export controls. The 2006 audit recommended that SAP implement tools to verify the location of users making download requests of SAP software. In 2010, the findings of the internal audits, including the failure to implement IP blocking, were brought to the attention of SAP's Executive Board. In 2014, the audit specifically recommended the implementation of geolocation IP address screening as a corrective measure. Though SAP knew of this compliance vulnerability since 2006, and despite being aware that its U.S.-based content delivery provider had the ability to conduct geolocation IP address screening years earlier, SAP failed to implement the recommended geolocation IP address screening until 2015. IP address data reviewed during the course of SAP's internal investigation confirmed that SAP software was being downloaded by users in Iran.

The Apparent Violations related to the sale of SAP software to pass-through entities were also enabled by SAP personnel. Internal communications show that SAP product line and overseas subsidiary managers oversaw the sale of SAP software and services from the United States or U.S. persons to pass-through entities knowing they would provide the software and services to Iranian companies. In one instance, SAP personnel traveled to Iran to secure SAP software sales.

Additionally, SAP failed to conduct sufficient due diligence on SAP Partners, which could have revealed SAP Partners' connections to Iranian companies. For instance, SAP Partner websites publicized their business ties with Iranian companies. SAP also failed to adequately investigate whistleblower allegations it received between approximately July 2011 to March 2016 that claimed SAP software had been sold to Iranian front companies registered in UAE, Turkey, and Malaysia, claims that SAP subsequently substantiated.

Cloud-Based Software Sales

Additional Apparent Violations occurred when SAP's cloud business group (CBG) subsidiaries in the United States sold cloud-based software subscription services to customers that enabled access to employees or customers in Iran. These exports occurred partly as a result of a failure to timely integrate the CBG subsidiaries into SAP's broader compliance structure. In 2011, SAP had begun acquiring several U.S.-based CBGs that operated internationally. Pre- and post-acquisition due diligence on the CBGs found that they generally lacked comprehensive export controls and sanctions compliance programs, and in some instances had no sanctions compliance measures at all. Despite these findings, SAP permitted the CBGs to continue operations as standalone entities without fully integrating them into SAP's existing compliance measures. SAP instead relied on its small U.S.-based Export Compliance Team to coordinate and enforce compliance processes for the CBGs. The U.S.-based Export Compliance Team was not resourced or empowered to manage these processes appropriately. These processes, moreover, were not consistent across all the CBGs due to

technological challenges and encountered resistance from some CBGs that did not view sanctions compliance as necessary. The Export Compliance Team reported these challenges to SAP's Germany-based compliance team, but received limited support. SAP compliance deficiencies within the CBGs were not appropriately addressed until September 2017.

Penalty Calculations and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $56,025,470. OFAC determined, however, that SAP voluntarily self-disclosed the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter is $1,316,157.

The settlement amount of $2,132,174 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be **aggravating factors**:

(1) SAP demonstrated reckless disregard and failed to exercise a minimal degree of caution or care for U.S. economic sanctions by failing to act upon the findings of multiple internal audits conducted over a period of at least eight years highlighting sanctions risks, as well as warnings from its compliance personnel indicating compliance program deficiencies that could lead to violations of U.S. economic sanctions regulations. SAP also ignored other warning signs, including whistleblower claims alleging sales of SAP software from the United States to Iran. It further permitted its U.S.-based CBGs to operate as standalone entities despite pre- and post-acquisition due diligence and reports from its U.S.-based Export Compliance Team notifying SAP headquarters of significant compliance deficiencies;

(2) SAP also acted recklessly by having a compliance program that was not commensurate to SAP's size and sophistication and that did not: 1) implement adequate controls in a timely manner (e.g., instituting geo-location IP address screening for SAP software delivered from the United States); 2) conduct an adequate degree of due diligence on SAP Partners; and 3) implement robust controls or compliance requirements for SAP Partner sales and SAP CBGs;

(3) SAP had direct knowledge or reason to know that SAP software and cloud services were being sold or used by entities and end-users in Iran and were supported from the United States. In some cases, SAP managers and other personnel had direct knowledge and facilitated the purchases of SAP software by third-country entities that enabled the use of SAP products in Iran. SAP had reason to know, from IP address data, that SAP software, updates, and services were being downloaded from the United States by end-users located in Iran. In addition, information posted on SAP Partners' websites publicized business ties with Iranian companies;

(4) SAP's exportation from the United States of business enterprise software and services to Iran caused harm to U.S. sanctions program objectives and undermined U.S. policy

objectives by providing economic benefit to Iran, including the provision of leading business enterprise software in the amount of $3.9 million to be used by Iranian businesses; and

(5) SAP is a sophisticated software company with significant international operations and has numerous foreign subsidiaries.

OFAC determined the following to be **mitigating factors**:

(1) SAP has no prior OFAC sanctions history, including no penalty notice or Finding of Violation in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations;

(2) SAP substantially cooperated with OFAC's investigation, including arranging interviews with SAP employees;

(3) SAP took significant remedial actions, including:

- Terminating all users associated with the third-country entities that provided software and services to Iran, and Iranian cloud services;
- Terminating SAP Partners engaged in sales to Iranian companies;
- Blocking all downloads of software, support, and maintenance from Iran and other embargoed countries;
- Implementing a risk-based export control framework for SAP Partners that requires a stringent review of proposed sales by a third-party auditor;
- Developing and implementing an improved compliance program, including geolocation IP screening;
- Hiring more than six new employees responsible for export control and trade sanctions compliance; and
- Terminating five employees found to have knowingly engaged in the sale of SAP products to Iran or failed to adhere to SAP internal policy prohibiting sales to embargoed countries.

Compliance Considerations

This enforcement action highlights for global companies providing software products online, including through cloud-based services, direct downloads, or other such means, the importance of implementing a risk-based sanctions compliance program commensurate with their size and sophistication and appropriate to their marketing and operational structures. Screening processes for such programs will generally include IP address identification and blocking capabilities and are especially important for companies that use sales models where engagement with the end-user is indirect. Such companies include those using third-party vendors or distributors for product delivery, or who deliver services to customers who might provide them to employees or other users. As in other industries, due diligence for software distributors, resellers, and agents is essential.

This enforcement action also emphasizes the importance of conducting sufficient pre- and post-acquisition due diligence to identify and promptly remediate compliance deficiencies in newly

acquired subsidiaries. Compliance efforts in such circumstances should be sufficiently resourced and empowered to undertake thorough examinations of risks and to implement appropriate controls, including, if needed, any stopgap measures.

OFAC sanctions compliance programs should further maintain the support and commitment of senior-level managers to be effective. In circumstances where senior-level managers are made aware of potentially violative conduct or compliance deficiencies, it is incumbent on them to take expeditious action to seek and abide by appropriate guidance.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that source goods or services from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The *Framework* also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The *Framework* includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

For more information regarding OFAC regulations, please go to: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.