

MISSION STATEMENT

CYBER-SECURITY BUSINESS DEVELOPMENT MISSION TO PERU, CHILE, AND URUGUAY WITH OPTIONAL STOP IN ARGENTINA

Dates: October 5-9, 2020

MISSION DESCRIPTION

The United States Department of Commerce, International Trade Administration (ITA), is organizing a Cybersecurity Business Development Mission to Peru, Chile, and Uruguay, October 5–9, 2020, with an optional stop in Argentina on October 13, 2020.

This mission aims to introduce U.S. firms and trade associations to some of South America's most rapidly growing information and communication technology (ICT), security, and critical infrastructure protection markets. It will assist U.S. companies in finding business partners to which they may export their products and services to the region. Target participants are U.S. companies and U.S. trade associations with members that provide cybersecurity and critical infrastructure protection products and services. The mission will visit Santiago, Chile; Montevideo, Uruguay; and Lima, Peru, along with an optional stop in Buenos Aires, Argentina. Participating firms will have the opportunity to gain market insights, make industry contacts, solidify business strategies, and advance their own specific projects, all with the goal of increasing U.S. cyber security product and service exports to the region. This mission will include customized, one-on-one, business appointments with pre-screened potential buyers, agents, distributors, and joint venture partners. It will also allow for meetings with industry leaders as well as state and local government officials, along with other networking events.

COMMERCIAL SETTING

Cybersecurity refers to the ability to protect or defend networks of information system infrastructures including the Internet, telecommunications networks, and computer systems from cyberattacks. Constantly evolving cyber risks and cyberattacks create a market for cybersecurity products and services for critical infrastructure protection, governments, and all sectors of the economy. The damaging effects of cyberthreats can reach all levels, ranging from businesses to individuals, and transgress national borders. Accordingly, authorities in countries in the South American region are currently dedicating an increased amount of resources to deal with these complex cyber threats in the public and private sector. Recent events and well-publicized cyberattacks in the region have also heightened the awareness of the importance of improving cybersecurity protection. Therefore, governments in the region, including Peru, Chile, Uruguay, and Argentina have made cybersecurity a policy priority, creating national task forces and/or increased attention on national cybersecurity strategies to improve their cybersecurity posture.

Recognizing that national and economic security depends on the reliable functioning of critical infrastructure, the U.S. National Institute of Standards and Technology (NIST) released the Cybersecurity Framework consisting of standards, guidelines, and practices for reducing cyber risks to critical infrastructure in February 2014 and released the latest updated version 1.1 in April 2018. The Framework, created through collaboration between industry and government,

consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

While the Framework was created in the United States, it provides an important standards-based approach that has been adopted by industries across the globe and lays the groundwork by which other governments have formulated their own frameworks and cybersecurity strategies. Private sector stakeholders have made it clear that the global alignment of cyber security protocol is important to avoid confusion and duplication of effort, or even conflicting expectations in the global business environment. These needs have been reiterated by multi-national organizations. Countries in South America are currently considering approaches compatible with the framework established by NIST. NIST has been holding discussions with several nations across the region, such as Brazil, Uruguay, Peru, and Colombia, making noteworthy internationalization progress in the cyber-security field. Uruguay has already adapted the Framework into their national cybersecurity policy. The potential adoption of important sections of NIST's Framework by industries such as healthcare, financial and other critical infrastructure sectors across South America can facilitate convergence, adoption and internationalization of a common risk-based approach to managing cybersecurity risk, which provides market access opportunities in the region to U.S. firms with cyber security expertise and solutions.

This trade mission also supports the Digital Connectivity and Cybersecurity Partnership, more commonly referenced as the "Digital Partnership" or "DCCP" which backs communications infrastructure development through private enterprise-led partnerships to promote transparent regulatory policies for open, competitive markets and, builds cybersecurity partnerships to address shared security threats. This model embodies fair competition and private investment, multi-stakeholder internet governance, interoperable ICT and strong cybersecurity practices.

This global, interagency initiative focused initially on the Indo-Pacific region but has since expanded to include the Western Hemisphere. The trade mission supports the DCCP in the Western Hemisphere by promoting the U.S. model of internet and ICT development, and especially strong cybersecurity best practices and a trusted Internet, in South America. Through business-to-business and government-to-government exchanges, the mission will contribute to catalyzing the DCCP by building connections, advancing an open Internet, growing global markets, and enhancing cybersecurity.

Peru

Peru's technological ecosystem is only now starting to take off which presents opportunities for U.S. providers of related goods and services. According to a World Bank report in 2017, approximately 49% of Peruvians (with a total population of approximately 32 million in 2019) use the internet compared to 25% in 2007.

Peru has greatly increased digital access over the past decade and efforts underway will continue to close the gap. Peru declared the construction of a national fiber optic backbone network as a national interest in 2012 with the policy goal of providing universal digital access. The country's fiber optic network was inaugurated in 2016, which covers over 13,000 km to provide broadband

service to 180 provincial capitals and connects 22 of Peru's 25 regions. The network is to serve as the backbone of future broadband regional networks in Peru. The government of Peru (GoP) has continued in this effort by expanding internet access through private concessions for the installation of broadband, awarding 13 concessions in 2017 and 2018. Broadband installation has been slow, as nearly all the concessions have multiple contractual amendments and delays.

The government is also in the process of expanding digital access in rural areas deep in the interior – via satellite connections and associated hardware installation. A current tender to link up to 2000 rural schools is in process. Likewise, Spain-based Telefonica and Facebook will launch a project to provide open-access, wholesale broadband mobile internet service to expand coverage in rural areas with funds from the Development Bank of Latin America and the Inter-American Development Bank (IDB) with the goal of covering 30,000 communities and reach six million Peruvians by 2021.

Opportunities for U.S. producers cyber/ICT goods and services are on par with that of other developing countries of its size. Recent corruption scandals have led to a stronger drive to clean up the tendering and procurement system, and it is here that U.S. companies have a particular advantage given their adherence to FCPA and known quality. Conversely, Peru is still hesitant to let go of the practice of selecting the lowest cost bidder for government contracts. This may in some cases apply to many of the big government infrastructure tenders/procurements emanating out of entities such as the Reconstruction Authority, ProInversion, and the Ministry of Transportation and Communications. Firms participating in the trade mission would have the opportunity to meet with:

- Private sector – partners and/or end users
- SEGDI - Secretaria Digital de Gobierno representative
- Vice Ministry of Communications Authority
- MinDEF relevant cyber side
- Peru Digital rep from MinEDU

SEGDI is in the process of developing policies to implement/deliver digital services across the government. SEGDI reported that it is in the process of establishing a Digital Security Center (despite limited resources – there are only 80 personnel in the unit). Working with AmCham, the embassy agreed to actively support SEGDI's digital transformation plan via training for relevant Ministry officials including SEGDI to be done in conjunction with interested U.S. technology companies.

Moreover, 32% of organizations in Peru suffered cyber-attacks over the last two years, a figure that highlights the need for a policy of prevention and data protection in organizations. Only 7% of organizations in Peru have a data protection policy, developed at the level of each department, which is constantly reviewed and improved. The need for quality cyber security policies and products and services is highlighted through the fact that 65% of organizations in Peru allocate between 1% and 5% of the IT budget for cybersecurity, while only 18% of organizations allocate a budget greater than 10%. Yet, organizations are increasingly aware that the human factor remains of vital importance for information security, so 80% of companies have a general

awareness program on cyber threats, of which only 7% were formal and focused, and 20% were tested and improved. These statistics highlight the needs and opportunities for U.S. cyber security products and services in Peru.

The GoP remains eager to learn from the United States on digital issues and how to apply best practices; and a number of workshop/conferences have been held to this effect. Likewise, the Peruvian Military is moving forward with its cyber defense and security plans. It remains open to meet with and learn about U.S. products and services.

The digitalism of the government has been identified as a priority, and measures to this end are already under way. The scope of this goal provides a large window of opportunity for private sector involvement, and in some cases, could help ease the workload of the government. With the expansion of internet access to rural areas and the renewed focus on strengthening cybersecurity, the Peruvian ICT sector is starting to establish itself as an emerging market in the region.

Chile

Although Chile has one of the highest levels of internet penetration in South America, with over 17 million broadband subscriptions in a population of over 19 million, the Chilean government had been slow to prioritize cybersecurity as a security issue. However, following a high-profile cyber security incident in 2018 at Banco de Chile, one of Chile's largest banks, which resulted in over \$10 million in losses, the Piñera administration declared cybersecurity a top priority.

With this new urgency, the Chilean Government has issued several new policies to strengthen their ability to protect and respond to cybersecurity threats. President Piñera has designated a new Presidential Advisor for Cyber-Security to create a more robust government entity to lead on cybersecurity efforts. The existing Chilean Computer Security Incident Response Team (CSIRT) under the Ministry of Interior has been given increased resources to monitor, detect, block, and communicate relevant cybersecurity threats for the government-owned infrastructure and websites. In addition, at a September 2019 Cybersecurity Symposium, Pamela Gidi, Undersecretary for Telecommunications, indicated that the Chile needs a boost in connectivity investments of at least 30% from \$1.5 billion to \$2 billion.

The United States is considered the partner of choice for the Chilean public and private sectors, which presents a unique opportunity for U.S. companies. U.S. cybersecurity solutions and NIST Cybersecurity Framework serves as the foundation for many Chilean private companies. The Chilean Commission for the Financial Market, the Chilean equivalent to the SEC, is using the Framework as a tool to develop cybersecurity standards to protect the country's financial system. The Secretaries of Defense of Chile and the United States signed an agreement in 2018 pledging closer cooperation in combating cyber threats. AmCham Chile is a founding member of the Alianza Chilena de Ciberseguridad, an industry association of key Chilean IT associations created to promote and develop cyber security in Chile through partnerships, education, and networking, and by cooperating with regulators and the government.

Chile is an ideal location to establish a regional office to take advantage of Santiago's position as a regional IT and financial hub and anticipated growth in cybersecurity spending across the continent. According to the consultancy firm P&S Intelligence, the South American cybersecurity market in 2017 was valued at US\$6.5 billion and is expected to grow to US\$22 billion by 2023. The Chilean market size is estimated at around US\$200 million for 2018, although that could increase as the country prepares to adapt to an increase in threats from high-profile IT infrastructure projects that could accompany the deployment of 5G and a planned submarine fiberoptic cable to connect Chile and East Asia.

Uruguay

According to the United Nation's 'e-Government Readiness Survey 2018', Uruguay is one of the most developed countries in Latin America in terms of e-commerce, e-government initiatives, and overall per capita internet penetration. The government of Uruguay is committed to digitizing all government services by 2020 through its "Digital Government Plan 2020", which includes single-sign-on mechanisms, digital signatures, filling out forms, and requesting appointments. In the Western Hemisphere, Uruguay only trails the United States and Canada in the E-Government Development Index.

The ICT sector is an important part of Uruguay's economy with software exports representing 12% of the country's \$3.5 billion in annual exports. Of these software exports, two-thirds are sold to the United States. Additionally, Uruguay's computer programmers are very sophisticated with many companies using Uruguayan computer professionals to support regional operations. Uruguay is also part of the "One Laptop Per Child Program," called Plan Ceibal, where all public-school children receive a laptop to augment their classroom experience and improve distance learning.

Despite the high level of information technology sophistication, the IDB noted "cyberspace protection efforts have not kept pace with digitization, thus leaving Uruguay's cyberspace vulnerable to attack." In the IDB's report called 'Strengthening Cybersecurity in Uruguay' noted:

Uruguay has carried out numerous initiatives to protect its cyberspace, staking its position as one of the most advanced countries in Latin America and the Caribbean in terms of cybersecurity. Yet, as noted in the 2016 Cybersecurity Report, significant weaknesses remain. AGESIC launched the Computer Emergency Response Team (CERT.uy) in 2008 and the Government Security Operation Center (GSOC) in 2017. The technical capacity and technological equipment of CERT.uy have not kept pace with the demands of a rapidly changing digital world, nor does the GSOC have all the resources it needs to fulfill its purpose. The government, though, is committed to achieving a secure digital environment, as reflected in "Uruguay Digital Agenda."

The IDB further states that main challenges are the lack of operational capacity to monitor, detect, and respond to incidents, and the lack of trained cybersecurity professionals. Accordingly, the IDB approved a USD \$10 million loan that will support the strengthening of Uruguay's capacity to protect its digital space by improving its systems to prevent, detect, and respond to cyber-attacks. One consultant noted that Uruguay needs at least 600 more cybersecurity

professionals to meet the current demand. Trade mission participants would have the opportunity to meet with entities such as:

- Private sector – partners and/or end users
- AGESIC – Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento Vice Ministry of Communications Authority
- CND – Corporacion Nacional Para el Desarrollo
- Banking Association
- Uruguayan Chamber of Information Technology
- State-owned utility companies

Argentina (optional stop)

A democratic change in government occurred in Argentina in December 2019. The priorities of the new administration should be evident within the first six months. The optional addition of Buenos Aires is a convenient opportunity to meet with industry players such as Google, Amazon, Motorola, and Cisco to better understand the new state of the ICT industry in Argentina.

IT Services offer major opportunities in network implementation, management and maintenance, legacy applications, wireless LANs, RTE (real-time infrastructure) implementations, remote operation processing, back-up, critical mission services, disaster recovery systems, Internet and network security systems, document digitalization, digital asset management, storage, utility computing, and information systems for rural areas. Cloud computing and virtualization-related services should continue to have high demand in 2020. The outsourcing of software development and call/contact centers is expected to see new investments, exports, and increased sales in the domestic market due to the January 1st, 2020 enactment of a tax incentive for the knowledge-based economy. The aim is to encourage knowledge-based and digital activities that result in manufactured products, services, or improved procedures.

Other market conditions are likely to foster growth in IT services, such as the increased use of e-banking, electronic commerce, and e-government, which have increased awareness related to information technology security.

Other Products and Services

The foregoing analysis of the cyber security opportunities in Peru, Chile, Uruguay, and Argentina is not intended to be exhaustive, but illustrative of the many opportunities available to U.S. businesses. Applications from companies selling products or services within the scope of this mission, but not specifically identified, will be considered and evaluated by the U.S. Department of Commerce. Companies whose products or services do not fit the scope of the mission may contact their local U.S. Export Assistance Center (USEAC) to learn about other business development missions and services that may provide more targeted export opportunities. Companies may call 1-800-872-8723, or go to <http://help.export.gov/> to obtain such information. This information also may be found on the website: <http://www.export.gov>.

MISSION GOALS

The purpose of this trade mission is to introduce U.S. firms to the rapidly expanding market for cyber-security products and services in South America. The mission will help participating firms and trade associations to gain market insights, make industry contacts, solidify business strategies, and advance specific projects, with the goal of increasing U.S. exports to Peru, Chile, Uruguay, and Argentina. By participating in an official U.S. industry delegation, rather than traveling to Peru, Chile, Uruguay, and Argentina on their own, U.S. companies will enhance their ability to secure meetings in those countries and gain greater exposure to the region.

MISSION SCENARIO

The business development mission will include one-on-one business appointments with pre-screened potential buyers, agents, distributors and joint venture partners; meetings with national and regional government officials, chambers of commerce, and business groups; and networking receptions for companies and trade associations representing companies interested in expansion into these South American markets. Meetings will be offered with government authorities that can address questions about policies, tariff rates, incentives, regulations, projects, etc.

PROPOSED TIMETABLE

***Note:** The final schedule and potential site visits will depend on the availability of host government and business officials, specific goals of mission participants, and ground transportation.

Sunday October 4, 2020	<ul style="list-style-type: none">• Trade Mission Participants Arrive in Lima, Peru
Monday October 5, 2020	<ul style="list-style-type: none">• Welcome and Country Briefing (Peru)• Presentations and/or cabinet/ministry meetings• Networking Lunch• One-on-One business matchmaking appointments• Networking Reception at Ambassador's residence (TBC)
Tuesday October 6, 2020	<ul style="list-style-type: none">• Travel to Santiago, Chile• Welcome and Country Briefing (Chile)• Presentations
Wednesday October 7, 2020	<ul style="list-style-type: none">• One-on-One business matchmaking appointments• Networking Lunch• Cabinet/ministry meetings• Networking Reception at Ambassador's residence (TBC)
Thursday October 8, 2020	<ul style="list-style-type: none">• (Morning) Travel to Montevideo, Uruguay• (Afternoon) Welcome and briefing• Presentations by Uruguayan government entities
Friday October 9, 2020	<ul style="list-style-type: none">• (Morning) Business matchmaking• Closing Ambassador's reception (TBC)• (Afternoon) Trade mission participants depart for optional Argentina stop or return home.

Saturday-Monday October 10-12, 2020	<ul style="list-style-type: none"> • Travel day or free time for Argentina optional stop participants. • National Holiday (Argentina) on Monday, October 12th
Tuesday October 13, 2020 (Optional)	<ul style="list-style-type: none"> • Welcome and Country Briefing (Argentina) • One-on-One business matchmaking appointments

PARTICIPATION REQUIREMENTS

All parties interested in participating in the trade mission must complete and submit an application package for consideration by the Department of Commerce. All applicants will be evaluated on their ability to meet certain conditions and best satisfy the selection criteria as outlined below. A minimum of 12 and maximum of 15 firms and/or trade associations will be selected to participate in the mission from the applicant pool.

FEES AND EXPENSES

After a firm or trade association has been selected to participate on the mission, a payment to the Department of Commerce in the form of a participation fee is required. The participation fee for the business development mission will be \$5,700 for small or medium-sized enterprises (SME)¹; and \$7,750 for large firms or trade associations. The fee for each additional firm representative (large firm or SME/trade organization) is \$1,000. The cost for the optional stop in Argentina is not included and is charged as a full Gold Key Service fee at an additional \$950 per small, \$2,300 per medium, and \$3,400 per large firm and trade association/organization, plus any direct costs.² Expenses for travel, lodging, meals, and incidentals will be the responsibility of each mission participant. Interpreter and driver services can be arranged for additional cost. Delegation members will be able to take advantage of U.S. Embassy rates for hotel rooms.

If and when an applicant is selected to participate on a particular mission, a payment to the Department of Commerce in the amount of the designated participation fee below is required. Upon notification of acceptance to participate, those selected have 5 business days to submit payment or the acceptance may be revoked.

Participants selected for a trade mission will be expected to pay for the cost of personal expenses, including, but not limited to, international travel, lodging, meals, transportation, communication, and incidentals, unless otherwise noted. Participants will, however, be able to take advantage of U.S. Government rates for hotel rooms. In the event that a mission is cancelled, no personal expenses paid in anticipation of a mission will be reimbursed. However, participation fees for a cancelled mission will be reimbursed to the extent they have not already

¹ For purposes of assessing participation fees, an applicant is a small or medium-sized enterprise (SME) if it qualifies under the Small Business Administration's (SBA) size standards (<https://www.sba.gov/document/support-table-size-standards>), which vary by North American Industry Classification System (NAICS) Code. The SBA Size Standards Tool [<https://www.sba.gov/size-standards/>] can help you determine the qualifications that apply to your company.

² See <https://www.export.gov/article?id=CS-User-Fees> for the U.S. Commercial Service user fee schedule for Gold Key Service.

been expended in anticipation of the mission.

If a visa is required to travel on a particular mission, applying for and obtaining such a visa will be the responsibility of the mission participant. Government fees and processing expenses to obtain such a visa are not included in the participation fee. However, the Department of Commerce will provide instructions to each participant on the procedures required to obtain business visas.

Trade Mission members participate in trade missions and undertake mission-related travel at their own risk. The nature of the security situation in a given foreign market at a given time cannot be guaranteed. The U.S. Government does not make any representations or guarantees as to the safety or security of participants. The U.S. Department of State issues U.S. Government international travel alerts and warnings for U.S. citizens available at <https://travel.state.gov/content/passports/en/alertswarnings.html>. Any question regarding insurance coverage must be resolved by the participant and its insurer of choice.

CONDITIONS FOR PARTICIPATION

Applicants must submit a completed and signed mission application and supplemental application materials, including adequate information on their products and/or services, primary market objectives, and goals for participation that is adequate to allow the Department of Commerce to evaluate their application. If the Department of Commerce receives an incomplete application, the Department may either: reject the application, request additional information/clarification, or take the lack of information into account when evaluating the application. If the requisite minimum number of participants is not selected for a particular mission by the recruitment deadline, the mission may be cancelled.

Each applicant must also certify that the products and services it seeks to export through the mission are either produced in the United States, or, if not, are marketed under the name of a U.S. firm and have at least fifty-one percent U.S. content by value. In the case of a trade association or organization, the applicant must certify that, for each firm or service provider to be represented by the association/organization, the products and/or services the represented firm or service provider seeks to export are either produced in the United States or, if not, marketed under the name of a U.S. firm and have at least 51% U.S. content.

A trade association/organization applicant must certify to the above for all of the companies it seeks to represent on the mission.

In addition, each applicant must:

- Certify that the products and services that it wishes to market through the mission would be in compliance with U.S. export controls and regulations;
- Certify that it has identified any matter pending before any bureau or office in the Department of Commerce;
- Certify that it has identified any pending litigation (including any administrative proceedings) to which it is a party that involves the Department of Commerce; and
- Sign and submit an agreement that it and its affiliates (1) have not and will not engage in the bribery of foreign officials in connection with a company's/participant's involvement

in this mission, and (2) maintain and enforce a policy that prohibits the bribery of foreign officials.

In the case of a trade association/organization, the applicant must certify that each firm or service provider to be represented by the association/organization can make the above certifications.

SELECTION CRITERIA

Targeted mission participants are U.S. firms, services providers and trade associations/organizations providing or promoting U.S. products and services that have an interest in entering or expanding their business in the mission's destination country(ies). The following criteria will be evaluated in selecting participants:

- Suitability of the applicant's (or in the case of a trade association/organization, represented firm's or service provider's) products or services to these markets;
- The applicant's (or in the case of a trade association/organization, represented firm's or service provider's) potential for business in the markets, including likelihood of exports resulting from the mission; and
- Consistency of the applicant's (or in the case of a trade association/organization, represented firm's or service provider's) goals and objectives with the stated scope of the mission.

Balance of company size and location may also be considered during the review process.

Referrals from a political party or partisan political group or any information, including on the application, containing references to political contributions or other partisan political activities will be excluded from the application and will not be considered during the selection process. The sender will be notified of these exclusions.

TIMELINE FOR RECRUITMENT AND APPLICATIONS

Mission recruitment will be conducted in an open and public manner, including publication in the Federal Register, posting on the Commerce Department trade mission calendar (<http://export.gov/trademissions>) and other Internet web sites, press releases to general and trade media, direct mail, notices by industry trade associations and other multiplier groups, and publicity at industry meetings, symposia, conferences, and trade shows. Recruitment for the mission will begin immediately and conclude no later than **July 17, 2020**. The U.S. Department of Commerce will review applications and inform applicants of selection decisions on a rolling basis until the maximum number of participants is selected. Applications received after **July 17, 2020**, will be considered only if space and scheduling constraints permit.

CONTACTS

USA

Gemal Brangman
Senior Advisor, Trade Missions
Trade Events Task Force
Washington, DC
202-482-3773
Gemal.Brangman@trade.gov

Paul Matino
Senior International Trade Specialist
Baltimore, MD – USEAC
410-962-4539
Paul.Matino@trade.gov

Pompeya Lambrecht
Senior International Trade Specialist
Northern Virginia – USEAC
703-235-0102
Pompeya.Lambrecht@trade.gov

Peru

Leon Skarshinski
Commercial Officer
U.S. Embassy – Lima, Peru
Leon.Skarshinski@trade.gov

Chile

Joshua Leibowitz
Commercial Officer
U.S. Embassy – Santiago, Chile
Joshua.Leibowitz@trade.gov

Uruguay

Matthew Poole
Senior Commercial Officer
U.S. Embassy – Montevideo, Uruguay
Matthew.Poole@trade.gov

Argentina

Karen Ballard
Commercial Officer
U.S. Embassy – Santiago, Chile
Karen.Ballard@trade.gov