L-1 IDENTITY SOLUTIONS, INC.
Form 10-K
February 28, 2008

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 10-K

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the Fiscal Year Ended December 31, 2007

OR

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the Transition Period from to .

Commission File Number 001-33002

L-1 IDENTITY SOLUTIONS, INC.

(Exact name of registrant as specified in its charter)

Delaware

02-0807887 (State or other jurisdiction of
incorporation or organization) (I.R.S. Employer
Identification No.) 177 Broad Street,
12th Floor, Stamford, CT 06901 (Address of principal executive offices) (Zip Code)
Registrant's telephone number, including area code: (203)-504-1100

Securities registered pursuant to Section 12(b) of the Act: Common Stock $.001 par value NYSE

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by a check mark if the Registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes No

Indicate by a check mark if the Registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act. Yes No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference into Part III of this Form 10-K or any amendment to this Form 10-K.

Indicate by a check mark whether the Registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definitions of ''accelerated filer'', ''large accelerated filer'' and ''smaller reporting company'' in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer Accelerated Filer Non-Accelerated Filer Smaller Reporting Company

Indicate by a check mark whether the Registrant is a shell company (as defined in Rule 12b-2). Yes No

The aggregate market value of the voting stock held by nonaffiliates of the registrant as of June 29, 2007, was approximately $1,498.0 million.

As of February 22 2008, the registrant had 75,238,515 shares of Common Stock outstanding.

---

L-1 IDENTITY SOLUTIONS, INC.

TABLE OF CONTENTS

Table of Contents

PART I

Item 1.

Business

In this Annual Report on Form 10-K, the words ‘‘L-1’’, the ‘‘Company’’, ‘‘we’’, ‘‘our’’, ‘‘ours’’, and ‘‘us’’ refer to L-1 Identi Solutions, Inc. and, except as otherwise specified herein, to our subsidiaries. Our fiscal year ended on December 31, 2007.

L-1 Identity Solutions, Inc. and its subsidiaries (‘‘L-1’’ or the ‘‘Company’’) provide a full range of identity solutions and services that enable governments, and businesses to enhance security, establish a true biometric-based identity, protect personal data and support various intelligence requirements. Our identity solutions and services offerings have four main areas of focus:

- Credentialing Solutions, part of our Identity Solutions segment, includes: production of passports, HSPD-12 common access cards, drivers licenses and credential verifications;
- Multi-biometric Solutions, also part of our Identity Solutions segment, includes: sale of fingerprint and palm print scanners, mobile fingerprint scanners, third party digital video cameras with embedded L-1 software, iris based capture devices (PIER, HIIDE), integrated multi-biometric (finger, face and iris) devices, biometric access control, automated biometric identification system (ABIS), system oriented architectural workflow and database management software and multi-modal algorithms including automated fingerprint and palmprint identification systems, automatic facial recognition systems both static (digital photo or mug shot) and dynamic (video) and automated iris recognition systems (AIRS);
- Enrollment Solutions, includes: provision of enrollment stations and software for fingerprinting and facial data collection and processing, which is part of our Identity Solutions segment, and fingerprint services for background checks for federal, state and local governments, which is part of in the Services segment;
- Intelligence Services, included in our Services segment, provide training, program management, security, technical development and IT support to the intelligence community.

We offer a full range of biometric solutions, including facial, fingerprint and iris recognition solutions and technologies, both hardware and software based, that enable our customers to deal with a single entity for a wide range of identity applications. Our solutions provide the means to collect, manage and use identity data and enable our customers to manage the entire life cycle of an individual’s identity for a variety of applications including civil identification programs, criminal identification, military applications, homeland security, including border management, and commercial applications. The market for identity protection solutions has continued to develop at a rapid pace. We believe that consumers of identity protection solutions are demanding end-to-end solutions with increased functionality that can solve their spectrum of needs across the identity life cycle. Our objective is to meet those growing needs by continuing to broaden our product and solution offerings, leveraging our existing customer base to provide additional products and services, expanding our customer base both domestically and abroad, and augmenting our competitive position through strategic acquisitions. We also provide comprehensive government consulting, training, security, technology development, and information technology solutions to the U.S. intelligence community.

The Company operates in two reportable segments: the Identity Solutions segment and the Services segment. The Identity Solutions segment provides credentialing solutions and biometric-based identity solutions to federal agencies, state and local government agencies, including law enforcement and departments of corrections, foreign governments and commercial entities, such as financial, casinos and health care institutions. Customers, depending on their specific needs, may order solutions that include hardware, equipment, consumables, software products or services or combine hardware products, consumables, equipment, software products and services to create a multiple element arrangement. Our Identity Solutions revenues include products and related services, which comprise hardware, components, consumables and software, as well as maintenance, consulting and training services integral to sales of hardware and software. The Services segment provides enrollment services to federal and state government agencies and commercial enterprises, including financial institutions,

Table of Contents

as well as comprehensive consulting, program management, information analysis, training, security, technology development and information technology solutions to the U.S. intelligence community. Depending upon customer needs, our services can be bundled with identity solution, product and services offerings to create multiple element arrangements. See ‘‘Reportable Segments and Geographic Information’’ included in Item 7 for financial information regarding our segments.

We evaluate our business primarily through operating and financial metrics such as revenues, operating income (loss), and earning before interest, depreciation and amortization, intangible asset impairments and in process research and development charges, and stock-based compensation expense (‘‘Adjusted EBITDA’’) and free cash flow.

Reorganization

On May 16, 2007, the Company adopted a new holding company organizational structure in accordance with Section 251(g) of the Delaware General Corporation Law (the ‘‘DGCL’’) in order to facilitate our announced convertible senior notes (the ‘‘Convertible Notes’’ or ‘‘Notes’’) offering and in order to facilitate the structuring of acquisitions. Pursuant to the reorganization, L-1 Identity Solutions, Inc., a Delaware corporation incorporated in April 2007 became the sole shareholder of its predecessor, L-1 Identity Solutions Operating Company (‘‘L-1 Operating Company’’, previously known as L-1 Identity Solutions, Inc., and originally incorporated in Delaware as Viisage Technology, Inc. in 1996 ). The reorganization has been accounted for as a reorganization of entities under common control and the historical consolidated financial statements of the predecessor entity represent the consolidated financial statements of the Company. The reorganization did not impact the historical carrying amounts of our assets and liabilities or our historical results of operations and cash flows.

The holding company organizational structure was effected pursuant to an Agreement and Plan of Reorganization (the ‘‘Merger Agreement’’) among L-1 Operating Company, the Company and L-1 Merger Co., a Delaware corporation and wholly owned subsidiary of the Company (‘‘Merger Co.’’). The Merger Agreement provided for the merger of Merger Co. with and into L-1 Operating Company, with L-1 Operating Company surviving as a wholly owned subsidiary of the Company (the ‘‘Merger’’). The Merger was consummated on May 16, 2007.

By virtue of the Merger, all of the outstanding capital stock of L-1 Operating Company was converted, on a share for share basis, into capital stock of the Company. As a result, each former shareholder of L-1 Operating Company became the owner of an identical number of shares of our common stock. Additionally, each outstanding stock option and warrant to purchase shares of common stock of L-1 Operating Company was automatically converted into a stock option or warrant to purchase, upon the same terms and conditions, an identical number of shares of the Company’s common stock. The conversion of the shares of common stock in the Merger occurred without an exchange of certificates. Accordingly, certificates formerly representing shares of outstanding common stock of L-1 Operating Company are deemed to represent the same number of shares of our common stock. Upon consummation of the Merger, our common stock was deemed to be registered under Section 12(b) of the Securities Act of 1934, as amended, pursuant to Rule 12g-3(a) promulgated thereunder. For purposes of Rule 12g-3(a), we are the successor issuer to L-1 Operating Company. Pursuant to Section 251(g) of the DGCL, the provisions of our certificate of incorporation and bylaws are substantially identical to those of L-1 Operating Company prior to the Merger. Our authorized capital stock, the designations, rights, powers and preferences of such capital stock and the qualifications, limitations and restrictions thereof are also substantially identical to those of the capital stock of L-1 Operating Company prior to the Merger. The directors of the Company are the same individuals who were directors of L-1 Operating Company prior to the Merger. The executive officers of the Company and L-1 Operating Company are the same.

In connection with the consummation of the Merger, the Company entered into an Assignment and Assumption Agreement with L-1 Operating Company. Pursuant to the terms of the Assignment and Assumption Agreement the Company assumed L-1 Operating Company's obligations under certain plans, arrangements and agreements of L-1 Operating Company and its subsidiaries relating to stock options, employment or compensation, and certain other agreements. The other liabilities and

Table of Contents

obligations of L-1 Operating Company, including contingent liabilities, were not assumed by the Company in the Merger and therefore continue to be the obligations of L-1 Operating Company. The assets of L-1 Operating Company were not transferred to the Company and therefore continue to be assets of L-1 Operating Company.

The Company has no operations other than those carried through its investment in L-1 Operating Company, except the financing operations related to the issuance of the convertible notes, and substantially all of its assets consist of its investment in L-1 Operating Company. At December 31, 2007, the Company's carrying amount of its investment in L-1 Operating Company approximated $1,255.0 million.

Recent Acquisitions and Financing Activities

Understanding the growth potential that the identity solutions market represents, we have sought to close the gap between the need (a better method of securing and protecting personal identities) and the ability for current industry participants to provide it due to a lack of professional management, infrastructure and capital resources. We used Viisage Technology, Inc. (now renamed L-1 Identity Solutions Operating Company) as the platform upon which to build an end-to-end identity solution provider to integrate multi-modal technologies into products and services to serve the need for biometric technologies by local, state, federal and international customers. With these objectives in mind, we consummated the transactions and acquisitions described below.

In December 2005, we issued and sold to Aston Capital Partners, L.P. (''Aston''), approximately 7.6 million shares of Viisage common stock resulting in gross proceeds to us of $100 million. Aston is an investment fund managed by an entity controlled by certain of our current senior executives. Under the investment agreement with Aston, $85 million of the proceeds was used to finance acquisitions.

In December 2005, we acquired Integrated Biometric Technology LLC (''IBT''), a leader in providing fingerprinting products, services and solutions to government, civil, and commercial customers that require criminal background checks and screening. Also in December 2005, we acquired the AutoTest division of Openshaw Media Group, a provider of automated web-based applicant testing technologies for state departments of motor vehicles and other credential issuing agencies.

In February 2006, we acquired SecuriMetrics, Inc. (''SecuriMetrics'') which develops, customizes and sells multi-biometric solutions using its proprietary iris recognition technology, typically consisting of multi-biometric capture devices bundled with proprietary software.

In August 2006, we acquired Iridian Technologies, Inc. (''Iridian'') which owns and licenses an extensive portfolio of intellectual property related to iris recognition technology.

Also in August 2006, we merged with Identix Incorporated (''Identix'') a provider of fingerprint, facial and skin biometric technologies, and related system components, as well as fingerprinting services which are critical to biometric capture and knowledge discovery in large scale identification management problems. The fingerprint services business of Identix has been integrated into the business of IBT.

In October 2006, we acquired SpecTal, LLC (''SpecTal'') which provides comprehensive consulting and security solutions primarily to the U.S. intelligence community.

Also in October 2006, we entered in a revolving credit agreement pursuant to which we can borrow up to $150.0 million, with the potential of increasing the facility to $200.0 million. Borrowings under the revolving credit

agreement have been primarily used to fund our acquisitions.

In February 2007, we acquired ComnetiX Inc. (‘‘ComnetiX’’), a Canadian company providing biometric identification and authentication technologies and solutions to private and public sector customers. The ComnetiX acquisition created an important presence for us in the Canadian market and added a highly-complementary base of customers to our portfolio, particularly within the law enforcement community.

Table of Contents

In May 2007, we issued $175.0 million of Convertible Notes, the net proceeds of which were used to prepay the then outstanding borrowings under our revolving credit facility.

In July 2007, we acquired McClendon LLC, (‘‘McClendon’’) and Advanced Concepts, Inc. (‘‘ACI’’), which provide technical, network security and professional services to the U.S. intelligence community.

In January 2008, we announced an agreement to acquire Bioscrypt Inc. (‘‘Bioscrypt’’), a Canadian company that is a leader in the enterprise access control market. The acquisition is subject to customary closing conditions, including the approval of the shareholders of Bioscrypt. This acquisition is expected to close during March 2008.

All acquired companies continue to deliver their individually branded solutions and services to their customers. Increasingly, however, the companies come together to provide integrated L-1 branded solution sets to customers across federal, civil, criminal and commercial markets, and to border management agencies.

Industry Overview

Biometric Markets and Trends

Biometrics is the measurement of unique, individual physiological or behavioral characteristics, such as fingerprints, palm prints, facial characteristics, iris and voice patterns, hand geometry and handwriting patterns, which can be used to determine or verify an individual’s identity. The biometrics industry offers technology that digitally captures and encodes these individual biometric characteristics and then compares that uniquely personal characteristic against previously encoded biometric data to determine or verify an individual’s identity. Biometric technology provides improved accuracy and security, convenient and cost-effectiveness compared to traditional identification methodologies.

More stringent security requirements and more mobile global populations is increasing demand for technologies that offer a reliable and efficient means to verify identity. Biometrics, with its focus on uniquely individual characteristics, addresses the limitations inherent in traditional identification and authentication processes, such as paper credentials, passwords, PIN codes and magnetic access cards. Biometrics provides a solution for a broad range of applications, including border management, national identification programs, immigration control, identity theft and critical infrastructure applications such as employee verification, access control and information systems protection. We believe that government and commercial entities will increasingly adopt biometric-enabled solutions to identity management.

Governments were the early adopters of biometrics and are currently the primary customers for the industry. At the local law enforcement level, biometric technology permits more efficient criminal booking and processing and also allows officers in the field to identify potential suspects more reliably and efficiently. Within the military biometrics are used for the verification and identification of military personnel and contractors and collection and processing of biometrics from non-military personnel for the purpose of identifying potential hostile persons. At the national level, governments throughout the world have taken steps to improve security in response to heightened concerns over public safety from the threat of terrorism. National governments have mandated increased spending on security measures, implemented new regulations and placed greater emphasis on technology to address growing security concerns.

Fingerprints have been the most widely used biometric and benefit from a substantial existing infrastructure that employs fingerprints for identification. Governments and law enforcement agencies around the world have already

created vast databases of fingerprints and classify and share fingerprints. According to the FBI, its criminal database alone contains the fingerprints of more than 50 million individuals. Other organizations throughout the world, including foreign governments and law enforcement agencies, other U.S. government agencies and state and local law enforcement agencies in the United States, also have established large fingerprint databases.

Table of Contents

While fingerprinting is expected to continue to be the most prevalent biometric technology in the near term, iris, face and palm print and other technologies are being adopted and combined with fingerprinting in multi biometric applications to provide an additional level of security and accuracy and to allow for increased flexibility for applications where fingerprints are not suitable.

The principal use of biometric technologies in identification applications revolves around the use of biometrics in large scale databases for establishing uniqueness of identity. The process works by capturing a set of biometric samples of an individual and submitting it to a biometric search engine which is able to rapidly compare the submitted biometric sample against large databases of known identities. Initially these systems were referred to as Automated Fingerprint Identification Systems (AFIS). These were originally developed for large applications by agencies such as the FBI and Scotland Yard to facilitate criminal investigations, but since have grown into the civil markets and achieved widespread acceptance within national civil programs, where they are used to prevent identity fraud in national ID programs. In more recent years, the trend has evolved into a multibiometrics system capability, where the search engine is able to search not just fingerprints but simultaneously other biometric modalities notably face and iris. In response we have developed our Automatic Biometric Identification System (‘‘ABIS’’), which we sell to government agencies throughout the world for the civil and criminal applications. Our ABIS system is a scalable standards-based multi-biometric platform, offering flexibility that enables deployments in a wide variety of identification environments.

ABIS deployments vary widely in size, cost and complexity. In a local law enforcement deployment, the ABIS may be entirely contained within a single facility, with one or more capture devices attached to local computers, networked to a low-cost, small scale system capable of searching up to tens of thousands of records. The same system could be scaled up in large applications to consist of hundreds of biometric acquisition stations and millions of biometrics records.

The widespread deployment of ABIS-type systems and the development of biometric technologies to support the identification market have been among the biggest contributors to the growth of the biometrics industry. This growth is being driven by the increase in the worldwide demand for identity based security systems, where the goal is to combat identity fraud, to fix identity, and to grant identities privilege based on the level of trust that they earn through the background checking process.

Government-issued credentials serve as the primary means for confirming the physical identity of an individual. The effectiveness, however, of these credentials can be impaired because they can be counterfeited or altered, issued under false pretenses and historically have rarely been linked to an identity database. Failure to provide adequate identification protection can lead to breaches of security and identity theft, the consequences of which can range from national security threats and loss of life to significant economic loss. Within this context, we believe that there is increasing pressure on governments and businesses to accelerate the adoption of advanced technology identity solutions.

In addition to upgrading their security features, we believe that monitoring authorities at places like border entry points will increasingly embrace the use of automated document authentication technology to confirm the authenticity of presented credentials. Issuing authorities are increasingly incorporating biometrics to verify personal identities and deter fraud. While identity credentials are becoming more secure, the ability to obtain them under false pretenses continues to be a major weakness of the credential issuing process. As a result, issuing authorities are now focusing on improving their ability to verify the identity of a person requesting an identification credential prior to issuing that credential. As part of this effort, many authorities also have recognized the need to have secure and accurate documentation of the issuance process and supporting documents for each credential.

Internationally many countries have established or are establishing national identification, passport programs and voting systems and many of these systems are expected to utilize biometric technologies. Some of these programs are also aimed at helping to secure a country's borders by tracking entry and exit of both citizens and visitors and identifying potential terrorist threats. The United States established legislation requiring biometric identifiers to be included in the passports of

Table of Contents

current Visa Waiver countries (countries where citizens are not required to obtain a Visa prior to entering the U.S.). We offer a range of solutions, products and technologies that can be utilized in national identification, and/or passport and border crossing programs to enroll and verify citizens, visitors and potential threats and/or to add biometric identifiers to national identification and/or passport programs. Accordingly we believe that international markets provide an opportunity for revenue growth.

We believe the global market for advanced technology identity solutions is growing rapidly and is driven by the following key trends:

- Government-initiated security programs. We believe that the U.S. Federal Government and government agencies will continue to be key drivers for the growth and development of the market for advanced technology identity solutions by increasingly recommending, and in some cases mandating, the use of secure authentication as a key component of identity verification through such programs as:
  - the U.S. Visitor and Immigrant Status Indicator Technology program (''U.S. VISIT''), which uses biometric data as part of new screening procedures for non-U.S. citizens entering the United States;
  - the U.S. Department of State Passport Card program to issue a limited use passports in a wallet size format;
  - the Transportation Workers Identification Credential (''TWIC''), which is a credentialing program that may eventually cover an estimated 12 million national transportation workers;
  - the U.S. Department of State's ''contactless chips'' in passports, which are electronic chips that hold the bearer's biographic and photographic data;
  - the Transportation Security Administration's (''TSA'') Hazardous Material Threat Assessment Program (''HAZMAT''), mandating fingerprinting and security threat assessment of commercial truck drivers applying for, renewing or transferring the hazardous materials endorsement (''HME'') on their state-issued commercial drivers licenses (''CDL'');
  - the TSA's Registered Traveler Program (''RT'') under which the TSA will conduct a security assessment to determine eligibility of an individual for an expedited screening process at TSA security checkpoints. RT participants provide both fingerprint and iris biometrics, allowing either biometric to be used for positive identity verification at the airport;
  - Homeland Security Presidential Directive 12 (''HSPD-12''), which mandates that a common identification card be utilized by all Federal government employees and contractors. In 2004, the U.S. Federal Government issued the Federal Information Processing Standard for Personal Identity Verification of Federal Employees and Contractors as part of HSPD-12. HSPD-12 includes a requirement for document authentication in connection with the issuance of secure credentials to federal government employees; and
  - ID Act, signed into law in May 2005, which mandates authentication of a person's identity before they are issued a driver's license.
- Development of industry standards and requirements. Several organizations responsible for standards in a number of our markets have implemented requirements for the use of biometric recognition. For example, in May 2003, the International Civil Aviation Organization, which sets recommended travel document standards for its member states, selected face recognition as the biometric to be used in passport documentation. Moreover, in February 2003, the National Institute for Standards and Testing (''NIST'') which is part of the

6

Table of Contents

U.S. Department of Commerce, recommended that a dual system of fingerprint and face recognition technology be used to verify the identities of visa holders at points of entry in the United States. In addition, NIST has established a fingerprinting standard, referred to as Minutiae Extractions Standard or MINEX.

- Growing use of biometrics. Governments are increasingly mandating biometrics as an integral component of identity solutions. Global biometric revenue is projected to grow significantly driven by large-scale government programs and dynamic private-sector initiatives. Fingerprint is expected to have the largest share followed by face recognition and iris recognition.

- Increasing demand for background screening. Demand is growing from civil, state, federal and commercial fronts for background screening for applicants seeking a new job or individuals who provide services that require their identity to be vetted.

- Rising cost of identity theft and financial fraud. We believe the growing direct and indirect cost of identity theft and financial fraud is increasing the pressure on businesses and individuals to accelerate the adoption of advanced technology identity solutions. Identity theft is the nation's fastest growing crime.

- Convergence of physical and logical security systems. We believe that there is a growing need for governments and businesses to provide a highly secure, unified system for user authentication to access both physical assets, such as buildings, and digital assets, such as computer networks. For example, the U.S. Department of Defense's, or DoD, Common Access Card Smart Card program provides identity verification for approximately four million DoD employees and military personnel to enable access to military property and DoD computer networks. We believe that this program represents the model for identity protection solutions that will be implemented by governments and businesses in the future.

Government Services Markets And Trends

The federal government is the largest consumer of information technology services and solutions in the United States. We believe that the federal government's spending on information technology and services will continue to increase in the next several years, driven by the expansion of national defense and homeland security programs, the continued need for sophisticated intelligence gathering and information sharing, increased reliance on technology service providers, due to shrinking ranks of government employee technical professionals, and the continuing impact of federal procurement reform and Office of Management and Budget mandates regarding IT spending. Federal government spending on information technology has consistently increased in each year since 1980.

Across our core intelligence community customers, we believe the following trends will continue to impact spending and dependence on technology and support contractors:

- The emphases on irregular warfare, homeland defense, and combating the spread of weapons of mass destruction remain overarching guiding principles for current and out-year funding priorities. We believe intelligence agencies will increase demand for data and text mining solutions to enable them to extract, analyze, and present data gathered from the massive volumes of information available through open sources such as the Internet. This increased focus on national security, homeland security, and intelligence has also reinforced the need for interoperability among the many disparate information technology systems throughout the federal government. We believe the Department of Defense, Department of Homeland Security and the intelligence community will continue to be interested in systems that strengthen the coordination within and among agencies and departments.

- Although certain agencies within the intelligence community have indicated a goal of reducing reliance on contractors, the demand for

technology service providers is expected to increase due to the need for federal agencies to maintain core operational functions while the available technical workforce shrinks. Given the difficulty the federal government has

Table of Contents

experienced in hiring and retaining skilled technology personnel in recent years, we believe the federal government will continue to rely on technology service providers that have experience with government systems, can sustain mission-critical operations and have the required government security clearances to deploy qualified personnel in classified environments.

- In recent years, federal agencies have had increased access to alternative choices of contract acquisition vehicles-such as indefinite delivery/indefinite quantity (ID/IQ) contracts, Government Wide Acquisition Contracts (GWACs), the General Services Administration (GSA) schedule and agency specific Blanket Purchase Agreements (BPAs). These choices have created a market-based environment in government procurement. The environment has increased contracting flexibility and provides government agencies access to multiple channels to contractor services. Contractors' successful past performance, as well as technical capabilities and management skills, remain critical elements of the award process. We believe the increased flexibility associated with the multiple channel access, such as ID/IQ contracts, GWACs, GSA schedule contracts and BPAs, will result in the continued utilization of these contracting vehicles in the future, and will facilitate access to service providers to meet the demand for, and delivery of, required services and solutions.
- Once the level of involvement in Iraq and Afghanistan begins to wind down, the military role will likely evolve from less dependence on major combat operations to an increased use of precision strikes. Intelligence gathering, processing and analysis will become even more important to the mission of the commanders in the field. Future administrations may choose to pay for these activities through annual appropriations instead of supplemental funding. Going forward, it is expected that a substantial portion of the military budget will be needed to re-set and modernize equipment and infrastructure. We believe this will likely fuel a continuing demand for logistics services and network enabled mission capabilities that will provide an increasing level of performance efficiency while also introducing elements of cost-effectiveness.
- It is believed that the current strategic environment dictates the need for more dependencies in the form of alliances and partnerships. Alliances with large and small companies who have agency mission knowledge and/or established credentials related to specific solutions and services are critical in winning large contracts.
- The Office of Management and Budget (OMB) has issued a strategic sourcing directive to make business decisions about acquiring commodities and services more effectively and efficiently. In many cases, these strategies are designed to drive specific services to commodity status in order to leverage the government's purchasing power. Many of the multiple-award, ID/IQ contracts that typify today's market are derived from strategic sourcing initiatives that aggregate requirements and provide many options for users over extended performance periods.

Our Identity Solutions

Our identity solutions are intended to provide our customers with the customized products and services necessary to achieve the particular objective or address a specific customer need. An individual solution often includes multiple deliverables of hardware, equipment, consumables, software, right to additional software products, when and if available, related hardware maintenance, software maintenance, hardware repair or replacement, technical support services, training, installation and consulting services under a single arrangement. Our identity solutions incorporate modular components and services, including the following:

Multi-Biometric Capture and Live Scan Systems — Provide high quality images for multi-biometric recognition in the industry. We estimate that more than 15,000 systems are deployed worldwide for criminal and applicant processing, border management and enrollment into civil ID programs.

Multi-Biometric ABIS — Support finger, face and iris on a single platform. This biometric matching engine is used to eliminate duplicates and aliases in the U.S. State Department's visa

Table of Contents

issuance system and is also the main biometric search engine for the US Department of Defense enterprise database management and search solution.

Mobile Identification Systems — Use finger, face and iris biometrics for identifying subjects in the field. Our rugged and portable iris devices are deployed by the U.S. Department of Defense for overseas missions in Iraq, Bosnia, Afghanistan and other areas of conflict.

Facial Screening Systems — Alert customs and passport control agents when an individual on a watchlist attempts to enter the country. We supply the largest database solution for the Department of State with a database search of over 60 million facial records.

Information Security Software Solutions — Protect against unauthorized access to computers and networks. Our solutions are used by financial and health-care organizations around the world.

High-Quality Card Production Systems — Provide long-lasting, tamper-proof capabilities. Each year, we estimate that we enroll and produce more than 35 million individual credentials, such as U.S. passports and drivers' licenses, at more than 2,500 locations.

Document Authentication and Credentialing Systems — Encompass proofing, vetting, enrollment, biometrics, identity database management, card production and authentication components required to establish the authenticity of IDs in a large-scale secure credentialing program We estimate that more than 5,000 systems are deployed worldwide in over 25 countries

Fingerprinting Service Centers — Handle processing for employment and licensee applicants. We maintain the largest enrollment network in the country and process nearly one million applicants annually.

Government Technology and Security Services — Provide key expert assistance in counterterrorism, counterintelligence, homeland security, technology development, information technologies, vulnerability assessments and operational support to US government agencies. In addition, we provide expert processing and analysis of complex data sources in support to US government agencies.

Our solutions are designed to meet the ID needs of our customers. They combine industry-leading face, finger and iris recognition biometric technologies with state-of-the-art credentialing and document authentication capabilities and a range of outsourcing services to successfully meet all aspects of managing identity.

Federal and International Security Solutions

We seek to provide efficient and reliable products and services to help improve the security of nations and to protect their citizens, both at home and abroad. We have provided our solutions to all levels of government including every major U.S. government department and most U.S. military branches. We offer a comprehensive array of solutions that make it easier to implement civilian and criminal identification systems, border security programs and data protection measures. Our solutions respond to the federal and international identity needs and initiatives.

In the Identity Solution segment, we provide solutions, products or technologies in connection with the following:

- Homeland Security Presidential Directive 12 — Requires a common identification credential with Personal Identity Verification

(PIV) for federal employees and contractors. L-1 provides end-to-end capabilities for identity proofing as well as modular, customizable components and outsourcing services to ensure fast and easy compliance. Our offerings are GSA and NIST certified.

- Transportation Workers Identification Card — A program mandating a standardized secure credential containing biometric data for all transportation workers to enter into any secure area of a port.
- U.S. DoD Common Access Card — The standard identification credential for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel.

Table of Contents

- Registered Traveler Program — A nationwide private sector program designed to accelerate the screening process at participating airports for passengers who voluntarily choose to enroll by providing biometric fingerprint and/or iris data.
- US-VISIT Program (U.S. Visitor and Immigrant Status Indicator Technology) — An automated entry/exit tracking program that requires foreign visitors to submit biometric information upon arrival and departure to and from the U.S.
- Passport and Visa Issuance and Production — We supply and integrate the technologies, software, hardware, consumables and services to help with the identity enrollment, de-duplication and production of safer and more secure passports and other travel documents.
- Border Management Solutions — Our solutions offer a faster and more convenient process for travelers to pass through borders. They also empower border control officers to perform real-time searches against known watchlists and to scan more types of documents faster than ever before, helping to ensure that unwanted individuals do not enter the country. L-1's capabilities also enable the process of border management and control to happen seamlessly and with the same level of protection and security regardless of location, whether at a highly populated and wired checkpoint or a remote location connected wirelessly. We estimate that our biometric technologies and document authentication readers have been tested or deployed by border control agencies all over the world. Our companies have deployed more than 10,000 live scan systems, including for the U.S. Department of Homeland Security, for use at the nation's border crossings.
- SIRIS created for iris primary applications that call for fast and accurate identification. SIRIS is a high speed iris matching platform. Combined with portable and stationary iris devices, SIRIS offers end-to-end solutions for large scale programs.
- Frequent Traveler Solutions that speed processing times and ensure high-quality biometric capture every time for maximum verification accuracy and convenience for travelers.
- Watchlist Screening Solutions that seamlessly integrate into the immigration process to provide more accurate, real-time notification of possible matches against watchlists.
- Document Authentication Solutions that automate the reading and authentication of e-passport documents with contactless smart chips, as well as existing passports, driver's licenses and other ID cards.
- Mobile ID Solutions that allow for highly accurate and fast identification of individuals seeking to pass through borders at remote sites, land and sea crossings.

In the Services segment, we provide services in connection with the following:

- HAZPRINT — Requires focused background checks, including fingerprint-based biometric criminal history checks, for all commercial drivers who apply for, renew or transfer an endorsement to transport hazardous materials, including explosives.
- Department of Defense (DoD)/Intelligence Agencies – We help the DoD and Intelligence communities in the fight against terrorism across the globe by providing technology for insurgent registration, combatant identification, watchlist ID, credentialing and high security access control. Off the field, our solutions help agencies process background checks of military personnel faster in order to provide them with secure credentials and verify their identity for the purposes of issuing benefits or accessing secure facilities and networks. We provide scientific and technical solutions to the design, testing, and implementation of collection systems employed against the intelligence community's top tier hard-target intelligence issues. Our technicians design and deploy unique articles for situations

requiring concealment techniques and methodologies and provide training for field operations personnel. Our program management and technical services support assists the government in the definition and execution of large mission critical programs across the intelligence community.

Table of Contents

- Information Technology (IT) Solutions – We provide IT support to the intelligence community. Our core capabilities include: infrastructure engineering; systems engineering and integration; software development; and information assurance. We provide infrastructure engineering services supporting mission critical, high performance computing systems for national level intelligence customers. This expertise includes network architecture design, implementation of advanced network technologies, high performance computing including engineering and administration of supercomputers. Our expertise in systems engineering and integration covers requirements definition and analysis, selection/implementation of systems engineering methodologies/tools, program management support, system engineering and technical assistance (''SETA''), program scheduling/engineering review boards, configuration management, and supporting planning development, implementation, and delivery phases of projects. We also provide software engineering support to high visibility and critical intelligence missions such as signals exploitation and cryptanalytic processing. Information assurance services/solutions include tools development, threat analysis, database development, network traffic analysis, vulnerability analysis, risk assessment, and training.
- Geospatial Data – We are a supplier of support services for collection, analysis, and dissemination of geospatial data.

Federal, International, State and Local Criminal Solutions

Law enforcement agencies across the U.S. and internationally rely on us to provide solutions that help identify suspects and criminals faster and more accurately. With the power to scan millions of criminal records in seconds, and provide officers in the field with critical identity information in minutes, we are paving the way for a new era in identification for law enforcement agencies. Our companies have more than 20 years of experience serving the needs of law enforcement agencies. Our solutions include:

- Enrollment Solutions – a broad range of enrollment capabilities to integrate personal data with biometric information and credentialing products. The core of L-1 key capabilities, these solutions incorporate facial and iris biometrics with document printing and authentication.
- Next Generation Multi-Biometric ABIS – incorporates finger, face and iris recognition in a single platform to improve the speed and accuracy of criminal identification. Our solution is designed for maximum flexibility in the workflow for lower risk and greater return on investment.
- Booking Systems – help quickly identify known criminals at the booking process by capturing the highest quality biometric data.
- Mobile ID Solutions – offer immediate and highly accurate identity information on suspects to officers in the field. Our mobile ID systems, provide officers in the field with accurate identity information in minutes while saving time, enhancing officer safety and minimizing false arrests.