

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

Edgar Filing: L-1 IDENTITY SOLUTIONS, INC. - Form 10-K

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

Page	PART I	Item 1	Business	1	Item 1A	Risk Factors	25	Item 1B	Unresolved Staff Comments																							
36	Item 2	Properties	36	Item 3	Legal Proceedings	37	Item 4	Submission of Matters to a Vote of Security Holders	38	PART II																						
	Item 5	Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	39	Item 6	Selected Financial Data	41	Item 7	Management’s Discussion and Analysis of Financial Condition and Results of Operations	42	Item 7A	Quantitative and Qualitative Disclosures about Market Risk	69	Item 8	Financial Statements and Supplementary Data	71	PART III																
	Item 9	Changes in and Disagreements with Accountants on Accounting and Financial Disclosure	71	Item 9A	Controls and Procedures	71	Item 9B	Other Information	75	Item 10	Directors and Executive Officers and Corporate Governance	75	Item 11	Executive Compensation	75	Item 12	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	75	Item 13	Certain Relationships and Related Transactions and Director Independence	75	Item 14	Principal Accountant Fees and Services	75	PART IV	Item 15	Exhibits and Financial Statement Schedules	75	SIGNATURES	76	EXHIBIT INDEX	78

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 Identity 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,

1

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

2

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.

3

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.

4

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

5

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:

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. Visitor and

State Passport Card program to issue a limited use passports in a wallet size format;

- the U.S. Department of

Workers Identification Credential (“TWIC”), which is a credentialing program that may eventually cover an estimated 12 million national transportation workers;

- the Transportation

State’s “contactless chips” in passports, which are electronic chips that hold the bearer’s biographic and photographic data;

- the U.S. Department of

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

- 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

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

7

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

8

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

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.

- Registered Traveler

(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.

- US-VISIT Program

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.

- Passport and Visa

• 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.

10

Table of Contents

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.

- Information
- 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.

- 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.

- Investigation Systems – analyze finger and facial information found at crime scenes, leading to more IDs, regardless of the quality of the data found at the crime scene.

- Inmate ID Solutions – incorporates iris recognition to help establish fast and accurate identification at critical steps in the incarceration process from inmate booking to release.

- Jail Management System (JMS) – is an enterprise level biometrically enabled jail management system designed to manage a detention facility by streamlining the day to day operations and provide an easily customizable work flow process. The system manages every critical step in the incarceration process by providing customizable modules to handle everything from

pre-booking, classification, medical screening, housing, inmate funds and property, scheduling and movement, notification, release and many other critical functions. The JMS also seamlessly interfaces with a variety of external local, state, and federal ID systems.

11

Table of Contents

Our Civil Solutions

Producing valid and secure civil identity documents necessitates a wide range of requirements and each step of the process represents the potential for error and fraud that can compromise documents. We provide agencies, such as state departments of motor vehicles, with large-scale secure credentialing systems. We also maintain one of the largest anti-fraud visa issuance systems with the U.S. Department of State. Our solutions include:

Enrollment Systems – help to ensure the integrity of the ID with high quality biometric data capture, document authentication, and demographic data capture for integration with identity databases and human resources management software.

- Multi-Biometric

ABIS – incorporates finger, face and iris on a single platform to help prevent fraud in the issuance of secure documents, aids in the speedy identification of criminals and helps deter terrorists from obtaining ID documents or crossing borders.

Card Production and Document Authentication Systems – produce long-lasting, tamper-proof credentials.

- Verification

Solutions – are used to verify identities before credentials are issued and received.

- Drivers' License

Solutions – offer the latest in end-to-end processes for creating a consolidated verification of an identity claimed by an applicant. This is done through the integration of client and back-end software, services, document reader hardware, biometric technology and internal and external database queries.

Our Commercial Solutions

Protection of a business' valuable information and physical assets from identity theft, fraud and other security risks in today's high-tech operating environments demands a sophisticated security platform. Regulatory mandates that require proof of requisite steps taken to protect critical personal information is adding to the pressure. We offer the latest innovation in biometric technologies to vet an identity before an individual is hired or granted access to a company's data and physical assets. With it, we help companies better protect themselves from theft facilitated by a false or stolen identity. We provide solutions to:

- Financial

Services Firms – We help maintain the integrity of client records for new accounts, manage the background check process for prospective employees, and control access to secure facilities and online accounts.

- Healthcare

Organizations Companies – We preserve patient privacy and confidentiality of records by using biometrics to ensure that only authorized individuals have access to sensitive patient information. Our information security software helps healthcare organizations comply with the requirements set forth by the Health Insurance Portability and Accountability Act (HIPAA).

- Casino and Gaming –

We provide faster and more accurate background checks on prospective employees and offer improved biometric-based surveillance to identify known card counters and cheaters.

Our Services Offerings

Fingerprinting Services – The fingerprinting services experts at L-1 provide an accurate and quick means to process applicant data required in federal and state licensing programs. As a result, we can help get the identity information needed for agencies and organizations to make a hiring or licensing decision more quickly and accurately than ever before. Prospective licensee and employee fingerprints are captured quickly in a friendly, professional environment by one of our certified fingerprint technicians. The prints are taken using state-of-the-art live scan equipment that captures fingerprints without the use of ink and submits them electronically. As a result, our customers can receive criminal

12

Table of Contents

history results in days. Faster results mean licensing, or putting employees to work, more quickly and with peace of mind. Our fingerprinting services include:

- Live Scan

Fingerprinting – Applicants can call and schedule an appointment at a convenient location. Upon arrival, fingerprints are captured and submitted electronically the same day.

- Card Scan

Fingerprinting – This service allows applicants to capture fingerprints with ink and mail the cards to us. We convert the ink cards to an electronic format and submit the fingerprint records to the appropriate channeling agency within one business day.

- Onsite

Fingerprinting – This service brings our live scan systems directly to the customer’s location, helping fulfill short-term fingerprinting needs due to a large fingerprinting backlog, hiring surge or opening of new locations.

Our Government Technology and Security Services – Our government and security consulting services encompass the most pressing and sensitive areas of security and intelligence concerns facing the U.S. today. These service areas encompass but are not limited to, strategic initiatives, weapons of mass destruction, counterterrorism, proliferation, combat support, and homeland defense. Our three specific elements of service center on intelligence operations, sensor science and analysis, and information technology and include acquisition support, sensor design, program management, due diligence, information sharing and analysis, physical, technical and personal security, personnel surety, behavioral science, counterintelligence, vulnerability assessment, imagery analysis, forensic accounting, surveillance and surveillance detection, crisis management, computer forensics, operational support, network engineering, network architecture design, and information assurance.

Our professionals provide substantive analytic, scientific, technical expertise to some of our nation’s most critical missions in the IMINT, SIGINT, and MASINT, and combat support realms. We provide our customers with a unique and responsive capability based on our ability to provide tailored expertise to customer specific requirements world-wide. Our areas of specialization include full life-cycle acquisition, system engineering and integration, intelligence operations and analysis, sensor sciences and technical arts. Our experts can provide complete end-to-end services working along side the customer or we can provide management and consulting services as trusted agents of the customer.

Our personnel include all-source regional, functional, and technical analysts; field operations officers; trainers; software engineers; program managers; specialized government consultants; and operational support professionals. These individuals are veterans of the U.S. intelligence agencies, U.S. investigating agencies and the uniformed military services. Many are senior intelligence community leaders and recipients of numerous awards and commendations for their accomplishments and career services.

Clients served include:

- U.S.

Intelligence Community – Our group of intelligence professionals work at various locations across the intelligence community, assist in building operational and analytical programs and help to train and mentor the next generation of intelligence professionals. Our engineers, scientists, and intelligence analysts have footprints world-wide supporting the intelligence community. These individuals design, prototype, test, evaluate programs and materials, transition the results to operational projects and programs, and analyze the resulting data in support of intelligence community and DoD goals. The technical expertise of these professionals working alongside their government counterparts help

ensure mission success.

• Federal, State and Local Government Agencies – Our professionals offer expert consulting based on extensive technical and operational experience. We provide a wide range of analytical, linguistic, technical, scientific and other support to intelligence, defense, and law enforcement agencies. Our proven and cleared personnel can augment and/or provide technical support and specialized training in day-to-day operations.

13

Table of Contents

- Private Sector –

Based on extensive experience working with the government, we can provide physical and IT security assessments, identify security vulnerabilities both from internal and external threats, utilizing a unique approach of viewing security from the perspective of the “eyes of the attacker”, a proven and distinctive approach to identifying, measuring and mitigating risk. Our capability is founded on our employees, extensive experience working on counterterrorism, counterintelligence and security issues during their professional careers. Additionally, our technicians and analysts can advise and support of threat situations with sophisticated literal and non-literal real-time sensors allowing for safe monitoring of potential dangerous or hazardous activities.

Our Products and Technologies

We deliver solutions by leveraging our products and technology capabilities. We generally offer biometric, secure credentialing and documents authentication products and technologies that are bundled as part of a solution set. Our solutions may include one or more of the following components: hardware, software, consumables, equipment, maintenance, systems, IT and security services.

Biometrics:

Our biometric products and technologies include multi-biometric ABIS system. Live Scan booking, facial screening, fingerprint readers and scanners, iris recognition devices, mobile ID, inmate ID, access control, BioLogon® Software and ID tools/SDKs. Our products and technologies include:

Multi-Biometric Solutions

ABIS System is the scalable, standards-based and easy to integrate platform designed to help integrators and end users manage today’s criminal and civil ID challenges. Unlike closed end-to-end systems that are too risky and too expensive to develop and maintain, the ABIS System is an innovative back-end platform that helps minimize intervention in ID processes. The latest generation of our BioEngine fingerprint technology incorporates new and more accurate high-speed filters for fingerprint identification in increasingly larger populations and tests conducted by the US government place BioEngine in the top tier of fingerprint technologies.

LatentExaminer works with the latent finger lifts that are often very challenging, even for the most experienced latent examiner. Extensive edit and customization tools are available to assist in latent fingerprint identification. Once captured, the latent can be automatically or manually processed to optimize clarity for search submissions to the ABIS System.

FaceExaminer helps analyze, search, and identify faces of wanted subjects taken from Closed Circuit TV cameras and surveillance tapes. As a front-end module to the Identix Multi-Biometric ABIS system, the FaceExaminer is a powerful tool for enhancing the effectiveness and performance of face recognition environments, where the quality of the images is poor or the person may not be facing the camera directly.

TenprintExaminer is a multi-purpose tenprint image processing application capable of running on any Windows-based desktop computer. It provides extensive tools to analyze and manipulate tenprint images to enhance ABIS performance and maximize identification search rates. After a search, the TenprintExaminer provides extensive functionality to analyze and compare results.

TenprintVerifier/FaceVerifier are web-based, post-processing tools to assist in verification of transaction search results. Once a transaction has been completed, the verifier applications can display search results in a queue for

display and review in more detail. The queue of face, fingerprint, or other multi-modal search transactions can be searched based on your business process and policy requirements.

Workflow Manager offers unprecedented flexibility, giving the power to customize our ABIS system to customers' specific needs. The multi-biometric framework provides a single platform for finger, face and full hand biometrics for both criminal and civil environments, making it highly flexible.

14

Table of Contents

Iris Identification Solution from SecuriMetrics offers SIRIS which is a scalable enterprise level biometric matching platform that can be operated on a single laptop. Designed using architecture built for performance in raw matching speed and throughput capability, SIRIS operates with search speeds reaching over 1 billion matches per second; making country sized identification realistic. SIRIS is coined the Next Generation Iris Recognition Technology.

Live Scan Booking

Live Scan Booking provides multi-biometric capture solutions for maximum background check results and downstream matching performance. This includes the following products and systems:

Multi-Biometric Capture Station

- TouchPrint™

Enhanced Definition 3000 Live Scan Series

- TouchPrint™

Enhanced Definition 4100 Slap & Roll Live Scan

- TouchPrint™

Enhanced Definition 4800 Palm, Slap & Roll Live Scan

- TouchPrint™ Live

Scan Series Peripherals

Palm Scanner 4800 — the L-1 4800 Palm scanner provides the ability to go beyond a ten print or single finger scan to also allow for the easy capture of palm prints. The 4800 scanner provides easy, reasonably sized scanner to capture palms scans while maintaining ten-print and singer finger roll scans in a single platen device.

Facial Screening

FaceIt Argus is a real-time facial screening system that captures faces in live video stream from high resolution cameras, searches them against predefined watch lists, and generates alarms whenever a match is found. It enhances the efficiency of security and law enforcement personnel by providing a list of possible matches for human verification, so that the operator spends valuable time focusing on the persons of interest rather than the public at large.

Fingerprint Readers and Scanners

Forensic Quality Readers (DFR® 2080 & DFR® 2100/2130) are designed for large-scale enrollment and verification applications, these readers consistently capture high quality 500 ppi images for more accurate matching and faster processing. As a result, they help increase security with better authentication.

Commercial Readers (BioTouch® 500 USB) are designed for information security applications, these fast, durable, accurate and low-cost readers can help streamline the authentication process. Our 500 PPI optics are PIV certified and provide forensic quality images in a low cost package.

Mobile ID

HIIDE (Hand-held Interagency Identity Detection Equipment) is a full function, multi-biometric (iris, finger, face) enrollment, identification, and tracking device for use in a variety of applications including battlefield detainee

identification, corrections facilities, law enforcement, transportation workers identity, border control and healthcare.

PIER (Portable Iris Enrollment and Recognition) is a full function, hand-held iris recognition device used by various U.S. governmental agencies in the support of the war on terror, national security and homeland defense. The PIER is also deployed throughout the U.S. in detention facilities for fast and accurate inmate identification.

RDT4 is a solution that employs a modular handheld device that links to any pre-configured, supported PDA, taking advantage of today's smart-phone technology, and through a centrally located workflow manager can interface with various databases simultaneously, including the Identix ABIS®

15

Table of Contents

System. It combines this flexibility with forensic quality, autocapture fingerprint reader, the camera on the PDA, and a card reader module to scan documentation, such as a driver's license, to ensure more accurate IDs and time and cost savings for officers in the field.

Inmate ID

Offender ID (Iris) is an advanced secure identity management system incorporating state-of-the-art biometric technologies into an inmate identification system. Critical processes such as booking and release can now be securely executed with iris identification technology providing accurate inmate identification.

Access Control

FacePASS is a face recognition-enabled access control and security product used to conduct one-to-one verification of an individual's identity to authenticate that the holder of an ID document or token is the authorized user. The system carries out a real-time comparison between a live face and a stored reference image to confirm the identity of that person and grant respective rights and privileges while guaranteeing maximum reliability, security and efficiency. The system works fully automated, 24 hours a day without any user intervention and thus requires virtually no system administration after the installation.

BioLogon Software

BioLogon® is a multi-factor authentication solution which uses fingerprint biometrics to authenticate the identity of the person seeking access and to protect computers and networks from unauthorized entry. It is used by healthcare institutions in the United States and by banks across the world to manage privacy and secure assets.

ID Tools/Software Development Kits ("SDK")

ID Tools/SDKs combine proven, cutting edge technology with simple developer tools to create high performance solutions. They create innovative, high-performance biometric solutions and help deliver top performing solutions, interoperable and standards-compliant applications and faster turnaround with easy integration tools.

Secure Credentialing:

Our secure credentialing products, technologies and systems encompass proofing/vetting, enrollment, biometrics, identity database management, card production and document authentication systems. The products and systems offered include:

iA-Passport® processes travel and identity documents quickly and securely, working with iA-Authenticate®. The database is designed to recognize and automatically compare multiple, unique security features in each individual document type, as the unique database includes forensic information on passports, visas, U.S. Immigration cards, and national IDs.

Digital Image Workstations (ImageCAM™) provides standardized image capture for identity applications before enrollment and processing of finished driver's license(s) and identification cards. The system is unique to the driver's license industry with state-of-the-art digital image capture systems and workstation equipment for capturing, storing and electronically transferring cardholders' digitized images and demographic information.

The Toppan CP400 Printer is designed to produce secure smart cards and help prevent counterfeiting. Personalization data is reversed printed into a transfer film that is that is fused to the surface of the card using heat and pressure, and the unique indirect-transfer pigment ink technologies provide unique advantages in both quality and counterfeiting protection over dye-sublimation methods. The non-fading ink technology ensures outstanding durability against light and chemical reactions that cause images to fade.

16

Table of Contents

Viisage PROOF™ integrates client and back-end software, automated document authentication reader hardware and biometric technology, as well as internal and external database queries, to create a consolidated system for the verification of an applicant's identity. Viisage PROOF evaluates aggregated information on identification documents and the most commonly used breeder documents as well as a variety of additional data points, such as social security number and address verification, to produce a proofing confidence score that aids the credential issuing agency in the final decision about whether or not the candidate is allowed to proceed to the next phase of the identity solutions process or whether additional interviewing is required. This product is based on proprietary data analytics algorithms.

AutoTest™ is a web-based testing engine for the delivery and administration of randomized identity and domain knowledge tests. This system provides additional intelligence of a person's claimed identity prior to receiving a driver's license or other secure identity credential. Testing is conducted through departments of motor vehicles and automated web-based and kiosk applications.

AutoTest Scheduler™ is a web-based application used to automate the scheduling of knowledge and/or road tests for driver licensing. It also can be deployed over the Internet as a self-service application for customers to make appointments.

Document Authentication:

Our document authentication products, technologies and systems provide customers with invaluable tools for recognizing fraudulent identity documents and potential threats of all types. The products and systems include:

iA-thenticate® is a combined hardware and software solution designed to automatically authenticate documents, such as passports, visas, immigration cards, drivers' licenses, and military ID cards that individuals use as proof of their identity. The product helps governments secure their borders and businesses to reduce identity fraud by authenticating identity credentials through a process of scanning, image processing and data analysis.

ID-Suite™ offers detection of forged and altered state & government-issued ID cards in a variety of industries through software and services that provide additional layers of security to the iA-thenticate product line's authentication engine, as well as adding authentication capabilities for North American ID cards, such as driver's licenses, and adds magnetic stripe and barcode reading capabilities. The Suite includes:

iA-License™ — Comprehensive electronic database of North American ID templates for automated authentication of driver's licenses, military IDs and other identity documents.

- DL-Alert® — Reads, interprets, and verifies the content, sequence, and format of information encoded in the magnetic stripe and/or bar code of commonly used identity documents such as driver's licenses, state ID cards and military IDs.

- iA-Verify™ — Provides an additional security layer by applying sophisticated database queries to validate the issuance and biographic data read from driver's licenses, passports and other ID documents.

iA-thenticate® SmartChip is a combined hardware and software product designed to quickly and accurately read driver's licenses, ID cards and electronic passports used by travelers. It automatically reads and authenticates e-passport documents that contain contact-less SmartChips in just a few seconds.

ID-GUARD™ automatically scans document images and barcode/magnetic strip information from ID1 size documents and searches for and authenticates document security features using multiple light and angle sources. ID-GUARD® fits into small areas for use at service counters, office desks and is easily mounted for in-vehicle use. It is intuitive and works similarly to most office scanners and card swipe readers

Customers

Over 90% of our sales are to federal, state, local and foreign governments and government agencies. Contracts with governments and agencies generally allow the customer to terminate the

17

Table of Contents

contract for convenience of or for failure of the government to appropriate funds. For the year ended December 31, 2007, two U.S. federal government agencies, which we cannot name due to security considerations, accounted for 26% of L-1's revenues.

Historically, we have experienced minimal customer turnover. We believe this is a result of our strong product portfolio and emphasis on customer service and support. The following is a representative list of our customer base:

Security Solutions

- Department of Defense
- U.S. Intelligence Community
- Department of Homeland Security
- U.S. Department of State
- Office of Naval Research

Civil Solutions

- Arkansas Office of Driver Services
- Connecticut Department of Motor Vehicles
- Illinois Secretary of State
- Kentucky Transportation Cabinet
- Maryland Department of Transportation and Motor Vehicle Administration
- Mississippi Department of Information Technology Services
- North Carolina Department of Transportation
- North Dakota Department of Transportation
- Oklahoma Department of Public Safety
- Pennsylvania Department of Transportation
- State of Rhode Island, Department of Administration, Division of Motor Vehicles
- State of Delaware Department of Public Safety
- State of Montana, Montana Department of Justice, Motor Vehicle Division
- West Virginia Division of Motor Vehicles
- Wisconsin Department of Transportation
- Connecticut Department of Social Services

Border Management

- Pakistan National Database and Registration Authority
- Canada Customs and Revenue Agency
- U.S. Department of State
- Australia Customs

British Airport Authority
Finnish Frontier Guards
Defense Manpower Data Center
New Zealand Customs
U.S. Department of Homeland Security
Saudi Arabia Ministry of Interior
Brazil Department of Federal Police
Iceland

Criminal Solutions

City of New Bedford, Massachusetts Department
Police
Jefferson County, Alabama, Sheriff's Office
Kentucky State of Policy of the Commonwealth
of Kentucky
Ohio Department of Public Safety
Pinellas County Sheriff's Office
U.S. Army
Washington, D.C. Department of Corrections
Wisconsin Department of Transportation
California Department of Justice
Los Angeles County
Pennsylvania State Police
Texas Department of Public Safety
California Department of Corrections and
Rehabilitation

Commercial and Resellers

ABN AMRO Bank
Berlin Airport
Hanover Zoo
Casinos
Sentillion
Telos Corporation
NEC Solutions, Inc.
Sagem Defense Securities

Government, Technology and Security Services

U.S. Intelligence Community
Department of Defense
National Geospatial Agency

Fingerprinting Services

U.S. Transportation Security Administration
Florida Department of Financial Services
Illinois Department of Revenue
California Department of Insurance

California Department of Social Services
Michigan State Police
Missouri State Highway Patrol
Texas Department of Public Safety

18

Table of Contents

Business Development, Sales, Marketing, Bids and Proposals

We market our biometric solutions and services through a direct sales force, strategic partnerships and alliances. Our direct sales force is responsible for marketing and selling our entire identity solutions and services portfolio. We have a worldwide sales force responsible for delivering customer solutions and services to the North and South American markets, Europe, the Middle East and Asia Pacific. In addition, we have established a dedicated U.S. Federal sales team in Washington, D.C. responsible for marketing and selling to U.S. government agencies such as the Department of Homeland Security, the Department of State, the DoD and others. We also have a dedicated sales team responsible for driving sales to our worldwide customer base. We have a dedicated sales and services team operating from locations in Germany, the United Kingdom, Australia, UAE and Switzerland, strengthening our coverage and access to the international markets for our products, services and solutions. We have also realigned our marketing efforts to better coordinate the state and local marketing offerings of our divisions. Finally, we have established a team approach to pursuing intelligence agency opportunities to coordinate and provide a broader and stronger service offerings to the U.S. intelligence agencies. As of December 31, 2007, we employed 90 people in our business development and sales and marketing organization.

We also continue to seek to develop strategic partnerships and distribution channels to broaden our coverage and increase the size of our market worldwide. We have established original equipment manufacturer, or OEM, distribution agreements with partners to leverage our technologies. We have established channels of distribution for our document authentication products to open new markets outside of the U.S. Additionally, we work with systems integrators, solution providers and service organizations to deliver identity solutions in combination with their core capabilities to expand our access to such organizations' existing relationships, marketing resources and credibility in new markets. Local agents are also utilized to expand our international access to identity solutions opportunities around the world.

Our sales strategy is organized around specific markets: federal, state and local, international and commercial. Each sales organization is supported by functional groups, which design, engineer, manufacture, market, fulfill and support our market-specific offerings. Each of our sales organizations is further supported by a professional service group, which customizes solutions for each market, and a field service group to ensure ongoing performance of our systems at customer sites throughout the world.

Substantially all of our government services business and much of our solutions business is won through submission of formal competitive bids. Commercial bids are frequently negotiated as to terms and conditions for schedule, specifications, delivery and payment. With respect to bids for government work, however, in most cases the client specifies the terms and conditions and form of contract. In situations where the client-imposed contract type and/or terms appear to expose us to inappropriate risk, we may seek alternative arrangements or opt not to bid for the work. Our contracts and subcontracts are composed of a wide range of contract types, including firm fixed-price, cost reimbursement, time-and-materials, indefinite delivery/indefinite quantity (ID/IQ) and government wide acquisition contracts such as General Services Administration (GSA) schedule contracts.

Substantially all of our sales to new customers have been the result of competitive bidding for contracts pursuant to public sector procurement rules. In some cases, we may be competing with an entity that has a pre-existing relationship with a potential customer, which could put us at a significant competitive disadvantage. In other cases, however, we have pre-existing relationships with customers, which give us an advantage relative to our competitors for that customer. All material bids and proposals are subject to review and approval by senior corporate management prior to submission.

Sales and marketing costs were \$27.7 million, \$14.4 million and \$7.8 million for the years ended December 31, 2007, 2006 and 2005, respectively.

Research and Product Development

We have organized our research and development activities in what we believe, is an efficient model using centers of excellence distributed among our divisions. Our research and development

19

Table of Contents

team which totals approximately 180 developers, scientists and engineers, is distributed among focused centers of excellence that are maintained under the Company's divisions. Their activities are coordinated at the corporate level under the Company's chief technology officer to ensure support of the overall innovation goals and mission of L-1 and the realization of synergies in our research and development investment.

We focus our product development efforts on critical components for advanced technology identity solutions. These include proprietary software that addresses image capture, image processing, enhancement of face recognition, iris recognition, information retrieval from identity databases, document authentication, and the accuracy of searching and matching algorithms within very large databases. We believe our next generation fingerprint, facial, and iris recognition technology developments will be more reliable and cost effective than current commercialized technology, as well as provide additional functionality, including the storage of fingerprint and/or facial and iris templates on smart cards and similar storage devices. In addition, we focus on expanding our capabilities in solutions for the civil identification, criminal identification and border management markets.

We benefit from research and development activities conducted by the manufacturers of the components integrated into our systems such as cameras, database software and computers. Moreover, we perform research and development for our customers, including the U.S. government and its agencies.

For the years ended December 31, 2007, 2006 and 2005, research and development expense was \$18.5 million, \$11.6 million, and \$4.6 million, respectively. These amounts do not include spending for projects under research and development contracts, for which the related costs are included in cost of revenues.

Intellectual Property

We rely on patent, copyright, trademark and trade secrets and contract law to establish and maintain our proprietary rights in our technology products and manufacturing processes. The success of our business will depend in part on our proprietary technology and protection of that technology. While our intellectual property rights are important to our success, we believe that neither our business as a whole nor any segment of our business is materially dependent on any particular patent, trademark, license or other intellectual property right.

We have a portfolio of 152 U.S. and foreign patents. In addition, we have 76 U.S. and foreign patent applications in process for biometrics and document authentication technologies. While the duration of our patents varies, we believe that the duration of our patents is adequate relative to the expected lives of our products.

We have filed applications to register the trademarks of "L-1" and "L-1 Identity Solutions", and both applications have been approved for publication by the U.S. Patent and Office. We have a broad portfolio of other vital registered and pending trademarks in the U.S. and foreign jurisdictions.

Backlog

Backlog represents sales value of firm orders for products and services not yet delivered and, for long term executed contractual arrangements (contracts, subcontracts, and customer commitments), the estimated future sales value of estimated product shipments, transactions processed and services to be provided over the term of the contractual arrangements, including renewal options expected to be exercised. For contracts with indefinite quantities backlog reflects estimated quantities based on current activity levels. Backlog will not necessarily result in future revenue because firm orders may be cancelled, firm orders from governmental agencies may remain subject to funding options, renewals may not be exercised by the customers, and the quantities ordered, the volume of transaction

processed or services to be provided may be less than estimated. Backlog includes deferred revenues. Contractual arrangements could be cancelled by our customers without penalty for lack of performance. Contracts terminated by our customers for convenience generally would result in recovery of actual costs incurred and profit, if any, on work performed through the date of cancellation.

20

Table of Contents

At December 31, 2007 backlog, determined as described above, approximated \$715 million, of which \$400 million is estimated to be realized in the following twelve months. At December 31, 2006 backlog was approximately \$523 million.

Competition

The market for our identity solutions and services is extremely competitive and we expect this competitive environment to intensify as the market for our products and services continue to grow and mature. We compete on the basis of the following factors: technology, service and support, product quality, price, reliability, capability to work with large criminal history networks and flexibility in accommodating customer technical and business needs. We believe our ability to provide multi modal identity solutions incorporating finger, face and iris technologies, together with search and matching software to work with large databases differentiates us from our competitors.

The markets for our biometric products and solutions are characterized by rapid technological change as a result of technical developments exploited by competitors, the changing technical needs of the customers, and frequent introductions of new features. We expect competition to increase as other companies introduce products that are more price competitive, that may have increased performance or functionality, or that incorporate technological advances not yet developed or implemented by us. In order to compete effectively in this environment, we must continually develop and market new and enhanced products at competitive prices, and have the resources to invest in significant research and development activities.

A significant number of established and startup companies are developing and marketing solutions and related software and hardware for fingerprint, face, iris and other biometric security applications that could compete directly with our products. Some of these companies are developing ultrasonic, semiconductor or optically based contact fingerprint image capture devices. Other companies are developing and marketing other methods of biometric identification such as retinal blood vessel, signature recognition, hand geometry and voice. If one or more of these approaches were widely adopted, it would significantly reduce the potential market for our products.

We face competition from a number of competitors who are actively engaged in developing and marketing biometrics or other security products, including AuthenTec, Inc., AssureTec Systems, Inc., Bundesdruckerei, Canadian Bank Note Company, Limited, Cogent Systems, Inc., Cognitec Systems Corporation, CrossMatch Technologies, Digimarc ID Systems LLC, Imageware Systems, NEC Corporation, Precise Biometrics AB, Rochford Thompson, SafLink Corporation, Sagem Inc., Sagem Morpho Inc., Secugen Corporation and 3M-AiT.

In our government services businesses, we operate in a competitive industry that includes many firms, some of which are larger in size and have greater financial resources than we do. We obtain much of our business on the basis of proposals submitted in response to requests from potential and current customers, who generally also receive proposals from competitors. Additionally, we face indirect competition from certain government agencies that perform services for themselves similar to those we provide. Our competitors include divisions of large defense contractors such as BAE Systems, Computer Sciences Corporation, General Dynamics, Boeing Corporation, Lockheed Martin Corporation, Raytheon Corporation, Northrop Grumman Corporation, and Science Applications International Corporation, as well as a large number of smaller U.S. government contractors with specialized capabilities, such as CACI International, Inc., Booz Allen & Hamilton, SRA International and Mantech International Corporation. Because of the diverse requirements of U.S. government customers, shortage of quality personnel and the highly competitive nature of large procurements, we frequently team with others to pursue contract opportunities. Competitors will, at times, team with us or subcontract to us in the pursuit of new business. We believe that the major competitive factors in our market are technical competencies, successful past contract performance, intelligence and

military work experience, price of services, reputation for quality and the experience and clearance level of our employees.

21

Table of Contents

Manufacturing

We engineer and design the hardware products we sell and develop the software embedded in the products. However, we limit our manufacturing activities to the assembly, repair, and testing of sub-assemblies and quality control of the manufacturing process. Our hardware is fabricated to our specifications by contract manufacturing partners. We believe this will permit rapid expansion of production capacity to meet any significant increase in product demand and minimize the cost associated with the expansion of our manufacturing capabilities. We believe that the cost of material and fabricated subassemblies will decline if manufacturing volumes increase.

We currently use certain components, sub-assemblies and finished products which are purchased from sole source suppliers. The partial or complete loss of supplies available from sole source or limited sources of supply or the delay in receiving supplies from these sources could result in delays in manufacturing and shipping products to customers and may require the incurrence of development and other costs to establish alternative sources of supply. While we attempt to maintain inventory on sole sourced components, it may take us several months to locate alternative supplies if required, or redesign our products to accommodate components from different suppliers.

Seasonality

Our business in general is not seasonal. However, because most of our government services revenue is earned on a time and material and fixed price level of effect basis, we are impacted by holidays and vacations our employees may take during the summer and holiday seasons. We are also impacted by the fiscal funding and appropriation cycles of our major customers. For example, the U.S. government's fiscal year ends on September 30 of each year, and it is not uncommon for government agencies to award extra tasks or complete other contract actions in the weeks before the end of the fiscal year in order to avoid the loss of unexpended fiscal year funds. Moreover, in years when the U.S. government does not complete its budget process before the end of its fiscal year, government operations typically are funded pursuant to a continuing resolution that authorizes agencies of the U.S. government to continue to operate, but traditionally does not authorize new spending initiatives. When much of the U.S. government operates under a continuing resolution, as occurred during the federal fiscal year ending September 30, 2007, delays can occur in procurement of products and services, and such delays can affect our revenue and profit during the period of delay.

Financial Information about Foreign and Domestic Operations and Export Sales

For the years ended December 31, 2007, 2006 and 2005, export sales were approximately \$29.0 million, \$14.6 million, and \$6.0 million, respectively. Foreign operations and export sales may increase in relative and absolute terms in the future due to our increased focus on markets outside the United States. See Note 12 to our consolidated financial statements for additional information.

Capital Requirements

Our capital requirements consist of significant capital expenditures for new secure credentialing contracts and working capital needs. For example, when we bid on new state drivers' license contracts, we must commit to provide up front capital expenditures in order to install systems necessary to perform under the contract. We expect to meet our requirements from operating cash flows, bank borrowings and to, a lesser degree, proceeds from stock option exercises. We expect to fund our acquisitions from operating cash flows and with issuance of debt and other securities.

In October 2006, we entered into an Amended and Restated Credit Agreement the (“Agreement”) by and among the Company, Bank of America N.A. (the “Bank”), Bear Stearns Companies Inc., Wachovia Bank, Credit Suisse, Societe Generale and TD Bank North, to amend and restate the credit agreement, dated as of August 16, 2006, by and between the Company and the Bank. The Agreement provides for a revolving credit facility of up to \$150.0 million, with the potential for up to \$50.0 million in additional borrowings. In order to borrow under the facility we are required to comply with certain covenants, some of which may limit the amounts borrowed or

22

Table of Contents

available. The Agreement provides that up to \$25.0 million of the total facility amount may be used for the issuance of letters of credit. As of December 31, 2007, our borrowing capacity under the revolving credit agreement was \$57.3 million.

Amounts borrowed under the Agreement bear interest for any interest period (as defined by the Agreement) at the British Bankers Association LIBOR Rate, plus a margin of 1.75% (subject to adjustment to minimum margin of 1.50% and a maximum margin of 2.00% based on the Company's indebtedness to EBITDA ratio described below), and must be repaid on or before October 19, 2011. We also have the option to borrow at a fluctuating rate per annum equal to the higher of (a) the Federal Funds Rate plus ½ of 1% and (b) the rate of interest in effect for such day as publicly announced from time to time by Bank of America as its "prime rate", with respect to base rate loans plus the margin described above. If we have not borrowed all available amounts under the facility, we must pay a commitment fee of 0.375 % per annum on such unutilized amounts.

On May 17, 2007, we issued \$175.0 million of Convertible Notes with a conversion feature which allows us the option to settle the debt either in shares of common stock or to settle the principal amount in cash and the conversion spread in cash or stock. The net proceeds of the Convertible Notes offering, net of deferred financing costs amounted to \$168.7 million of which \$69.8 million was used to repurchase our common stock pursuant to a prepaid forward contract. The remaining net proceeds of the Convertible Notes offering were utilized to repay outstanding indebtedness. The Convertible Notes and a related forward share repurchase transaction are described in "Management's Discussion and Analysis of Results of Operations and Financial Condition-Liquidity."

Environmental Protection Regulations

We believe that our compliance with federal, state and local environmental regulations will not have a material adverse effect on our financial position or results of operations.

Employees

As of December 31, 2007, we had 1,819 full time employees. None of our employees are covered by collective bargaining agreements. We believe that our relations with our employees are good.

Officers

Our executive officers are appointed by our Board of Directors and serve until their successors have been duly appointed and qualified.

Robert V. LaPenta, 62, has served as the Chairman of the Board since December 2005, President and Chief Executive Officer of L-1 since August 2006. Mr. LaPenta is the founder and Chief Executive Officer of L-1 Investment Partners, LLC, a private investment management firm. From April 1997 to April 2005, Mr. LaPenta served as President, Chief Financial Officer and a Director of L-3 Communications Holdings, Inc., which he co-founded in April 1997. From April 1996, when Loral Corporation was acquired by Lockheed Martin Corporation, until April 1997, Mr. LaPenta was a Vice President of Lockheed Martin and was Vice President and Chief Financial Officer of Lockheed Martin's Command, Control, Communications and Intelligence and Systems Integration Sector. Prior to the April 1996 acquisition of Loral, he was Loral's Senior Vice President and Controller, a position he held since 1991. He joined Loral in 1972 and was named Vice President and Controller of its largest division in 1974. He became Corporate Controller in 1978 and was named Vice President in 1979. Mr. LaPenta is on the Board of Trustees of Iona College, the board of directors of Core Software Technologies and the board of directors of Leap Wireless International, Inc.

Dr. Joseph Atick, 43, joined L-1 in August 2006 as Executive Vice President and Chief Strategic Officer effective with the merger of Identix with L-1. Prior to that, he served as President & Chief Officer of Identix since June of 2002. Prior to that, he had co-founded one of the original facial recognition companies, Visionics Corporation. Over the years, Dr. Atick co-founded and managed several companies focused on technology transfer and development, and has served as a technical

23

Table of Contents

advisor to many high-tech enterprises and organizations, including NATO. He had also led the Computational Neuroscience Laboratory at Rockefeller University and the Neural Cybernetics Group at the Institute for Advanced Study in Princeton, New Jersey. Dr. Atick holds a Ph.D. in Mathematical Physics from Stanford University.

James DePalma, 56, joined L-1 as Executive Vice President, Chief Financial Officer and Treasurer effective with the merger of Identix with L-1. He brings three decades of operational and finance experience in the defense and technology industries to his role within the company. Prior to joining L-1, Mr. DePalma was a founding partner of L-1 Investment Partners. Prior to the formation of L-1 Investment Partners, Mr. DePalma served as a consultant to L-3 Communications Holdings, Inc. and was chief executive officer of Core Software Technology, a leading software provider to the intelligence community and an equity investment of L-3 Communications Holdings, Inc.

Doni Fordyce, 48, joined L-1 as Executive Vice President of Corporate Communications effective with the merger of Identix with L-1. In August 2006 she was a founding partner of L-1 Investment Partners and brings two decades of senior executive and investment management experience to the company, serving most recently as chief executive officer, president and chief operation officer of Bear Stearns Asset Management (BSAM) Inc. Prior to that Ms. Fordyce was vice president of Goldman Sachs Inc. from 1986 to 1996 where she was one of the founders of the asset management business. She has also worked in IT solutions consulting, specializing networking, data management and printing for investment banks and financial institutions.

Mark S. Molina, 48, joined L-1 in August 2006 as Executive Vice President, Chief Legal Officer and Secretary in August 2006 effective with the merger of Identix with L-1. Prior to joining L-1, he was Executive Vice President, Chief Legal Officer and Secretary at Identix, which he joined as Vice President and General Counsel in 1999. Mr. Molina is a business and technology lawyer with over 20 years experience structuring and negotiating mergers, acquisition, dispositions, joint ventures, technology licenses, financings and investments. He has considerable experience with public offerings and private placements as well as SEC reporting compliance and obligations of publicly traded companies.

Joseph Paresi, 52, joined L-1 in August 2006 as Executive Vice President and Chief Marketing Officer effective with the merger of Identix with L-1. He was a founding partner of L-1 Investment Partners LLC. Mr. Paresi brings three decades of executive management, product development, and design engineering experience in the technology and defense industries to his role with the company. Prior to joining L-1 Investment Partners, he served as corporate vice president of product development for L-3 Communications and as president of L-3 security & Detection Systems from 1997 to 2005.

Vincent A. D'Angelo, 63, joined L-1 as Senior Vice President of Finance in August 2006 effective with the merger of Identix with L-1. Prior to that, he was a consultant for L-1 Investment Partners. Prior to that, Mr. D'Angelo was a senior audit partner with PricewaterhouseCoopers for more than 35 years where he was involved in all facets of the business, including client service, management, operations, governance, SEC filings, and mergers and acquisitions.

There are no family relationships among any of our executive officers and directors.

On April 23, 2007, the Company entered into an employee arrangement with Mr. Robert LaPenta, Jr., the son of the Company's Chief Executive Officer, to serve as Vice President, M&A/Corporate Development.

L-1's Internet Website

We maintain a corporate website with the address www.L1id.com. We are not including the information contained in our website, or incorporating it by reference into, this Annual Report on Form 10-K. We make available, free of charge through our website, our Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q and Current Reports on Form 8-K, and any amendments to these reports as soon as reasonably practicable after we electronically file such material with, or furnish such material to, the Securities and Exchange Commission. You may read

Table of Contents

and copy any materials filed with the SEC at the SEC's Public Reference Room at 100 F Street, N.E., Washington, D.C. 20549. Please call the SEC at 1-800-SEC-0330 for further information about the Public Reference Room. The SEC also maintains a website, www.sec.gov containing the reports, proxy and other information we file with the SEC.

Item 1A.

Risk Factors

This Annual Report on Form 10-K contains or incorporates a number of forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. These forward-looking statements are based on current expectations, estimates, forecasts and projections about the industry and markets in which we operate and management's beliefs and assumptions. Any statements contained herein (including without limitation statements to the effect that we or our management "believe", "expect", "anticipate", "plan" or similar expressions) that are not statements of historical fact should be considered forward-looking statements and should be read in conjunction with our consolidated financial statements and notes to consolidated financial statements included in this report. These statements are not guarantees of future performance and involve certain risks, uncertainties and assumptions that are difficult to predict. There are a number of important factors that could cause our actual results to differ materially from those indicated by such forward-looking statements. These factors include, without limitation, those set forth below. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties, including those not presently known to us or that we currently deem immaterial, may also impair our business. We expressly disclaim any obligation to update any forward-looking statements, except as may be required by law.

Risks Related to Our Business

We have a history of operating losses.

We have a history of operating losses. Our business operations began in 1993 and, except for 1996 and 2000, have resulted in pre-tax operating losses in each year, which in 2006 and 2007, include significant asset impairments and merger related expenses, amortization of intangible assets and stock-based compensation expense. At December 31, 2007, we had an accumulated deficit of approximately \$69.8 million. We will continue to invest in the development of our secure credential and biometric technologies, as well as government services.

We derive over 90% of our revenue from government contracts, which are often non-standard, involve competitive bidding, may be subject to cancellation with or without penalty and may produce volatility in earnings and revenue.

More than 90% of our business involves providing solutions, and services under contracts with U.S. federal, state, local and foreign government agencies. Obtaining contracts from government agencies is challenging and government contracts often include provisions that are not standard in commercial transactions. For example, government contracts may:

- include provisions that allow the government agency to unilaterally terminate the contract without penalty under some circumstances;
- be subject to purchasing decisions of agencies that are subject to political considerations;
- include bonding requirements;

onerous procurement procedures; and

- be subject to

cancellation or reduction if government funding becomes unavailable or is cut back.

- be subject to

Securing government contracts can be a protracted process involving competitive bidding. In many cases, unsuccessful bidders may challenge contract awards, which can lead to increased costs, delays and possible loss of the contract for the winning bidder. Protests, and similar delays, regarding

25

Table of Contents

any future government contracts of a material nature that may be awarded to us could result in materially adverse revenue volatility, making management of inventory levels, cash flows and profitability inherently difficult. Outright loss of any material government contract through the protest process or otherwise, could have a material adverse effect on our financial results and stock price.

Similar to federal government contracts, state and local government agency contracts may be contingent upon availability of funds provided by federal, state or local entities. State and local law enforcement and other government agencies are subject to political, budgetary, purchasing and delivery constraints which may result in quarterly and annual revenue and operating results that may be irregular and difficult to predict. Such revenue volatility makes management of inventory levels, cash flows and profitability inherently difficult. In addition, if we are successful in winning such procurements, there may be unevenness in shipping schedules, as well as potential delays and changes in the timing of deliveries and recognition of revenue, or cancellation of such procurements.

In addition, government contracts may specify performance criteria that must be satisfied before the customer accepts the products and services. Collection of accounts receivable may be dependent on meeting customer requirements, which may be unpredictable, subject to change by the customer, and not fully understood by us at the time of acceptance of the order, and may require the incurrence of unexpected costs that may be uncompensated and could negatively affect profit margins and our liquidity.

We derive a significant portion of our revenue from federal government customers, the loss of which could have an adverse effect on our revenue.

For the year ended December 31, 2007, two Federal Government agencies accounted for 26.0% of consolidated revenues. For the year ended December 31, 2006, three Federal Government agencies accounted for 31.0% of consolidated revenues. For the year ended December 31, 2005, one customer, the U.S. Department of State, accounted for 27.5% of our consolidated revenues. The loss of any of our significant customers would cause revenue to decline significantly and could have a material adverse effect on our business.

We may not realize the full amount of revenues reflected in our backlog, which could harm our operations and significantly reduce our future revenues.

There can be no assurances that our backlog estimates will result in actual revenues in any particular fiscal period because our clients may modify or terminate projects and contracts and may decide not to exercise contract options. Our backlog represents sales value of firm orders for products and services not yet delivered and, for long term executed contractual arrangements (contracts, subcontracts, and customer's commitments), the estimated future sales value of estimated product shipments, transactions processed and services to be provided over the term of the contractual arrangements, including renewal options expected to be exercised. For contracts with indefinite quantities backlog reflects estimated quantities based on current activity levels. Our backlog includes estimates of revenues that are dependent on future government appropriation, option exercise by our clients and/or is subject to contract modification or termination. At December 31, 2007, our backlog approximated \$715.0 million, \$400.0 million of which is estimated to be realized in the following twelve months. These estimates are based on our experience under such contracts and similar contracts, and we believe such estimates to be reasonable. However, we believe that the receipt of revenues reflected in our backlog estimate for the following twelve months will generally be more reliable than our backlog estimate for periods thereafter. If we do not realize a substantial amount of our backlog, our operations could be harmed and our expected future revenues could be significantly reduced.

Our quarterly results are difficult to predict, and if we miss quarterly financial expectations, our stock price could decline.

Our quarterly revenue and operating results are difficult to predict and fluctuate from quarter to quarter. Our operating results in some periods may be below or above the guidance we have provided

26

Table of Contents

and may not meet investor expectations. If this happens, the market price of our common stock could be adversely impacted. Fluctuations in our future quarterly operating results may be caused by many factors, including:

- The size and timing of customer orders, which may be received unevenly throughout a fiscal year;
- The mix of revenues between solutions and services;
- The application of new accounting standard or interpretations;
- Cancellation or modification of contracts or changes in contract estimates; and
- Contract performance delays.

We have a long sales cycle, which can result in significant revenue fluctuations between periods.

The sales cycle for our products is typically long and subject to a number of significant risks over which we have little control. As our operating expenses are based on anticipated revenue levels, fluctuations in the timing of sales can cause our operating results to vary significantly between periods. If revenue falls significantly below anticipated levels, our business and the market price of our stock would be negatively impacted.

Purchasing decisions for our products and systems may be subject to delay due to many factors that are outside of our control, such as:

- Appropriation of funds by governments;
- Political and economic uncertainties;
- Time required for a prospective customer to recognize the need for our products;
- Customers requirements for customized features and functionalities;
- Turnover of key personnel at existing and prospective customers;
- Customer internal budgeting process; and
- Customer internal procedures for the approval of large purchases.

We are subject to government regulation, and our failure to comply with applicable regulations could subject us to penalties that may restrict our ability to conduct our business.

We are affected by and must comply with various government regulations that impact our operating costs, profit margins and the internal organization and operation of our business. Our failure to comply with applicable regulations, rules and approvals could result in the imposition of penalties, the loss of our government contracts or our disqualification as a U.S. Government contractor, all of which could adversely affect our business, financial condition and results of operations. Among the most significant regulations affecting our business are:

control regulations;

Regulation, or the FAR, and agency regulations supplemental to the FAR, which comprehensively regulate the formation and administration of, and performance under government contracts;

Negotiations Act, which requires certification and disclosure of all cost and pricing data in connection with contract negotiations;

Practices Act; and

and executive orders restricting the use and dissemination of information classified for national security purposes and the exportation of certain products and technical data.

- export
- Federal Acquisition
- Truth in
- Foreign Corrupt
- laws, regulations

27

Table of Contents

These regulations affect how our customers and we can do business and, in some instances, impose added costs on our business. Any changes in applicable laws and regulations could restrict our ability to conduct our business. Any failure by us to comply with applicable laws and regulations could result in contract termination, price or fee reductions or suspension or debarment from contracting with the federal government generally.

Biometric technologies have not achieved widespread commercial acceptance and our strategy of expanding our biometric business could adversely affect our business operations and financial condition.

Part of our strategy is to enhance our leadership in biometric technologies. Pursuing this strategy involves risks. For instance, to date, biometric technologies have not gained widespread commercial acceptance. Although there has been more recent activity, there is no assurance that this activity will continue. Some of the obstacles include a perceived loss of privacy and public perceptions as to the usefulness of biometric products. Whether the market for biometric technologies will expand will be dependent upon factors such as:

- national or international events which may affect the need for or interest in biometric products or services;
- the cost, performance and reliability of the products and services and those of our competitors;
- customers' perception of the perceived benefit of biometric products and services and their satisfaction with the products and services;
- public perceptions of the intrusiveness of these biometric products and services and the manner in which firms are using the information collected;
- public perceptions regarding the confidentiality of private information;
- proposed or enacted legislation related to privacy of information; and
- marketing efforts and publicity regarding these products and services.

We do not know when, if ever, biometric products and services will gain widespread commercial acceptance. Certain groups have publicly objected to the use of biometric products and services for some applications on civil liberties grounds and legislation has been proposed to regulate the use of biometric security products. From time to time, biometric technologies have been the focus of organizations and individuals seeking to curtail or eliminate such technologies on the grounds that they may be used to diminish personal privacy rights. If such initiatives result in restrictive legislation, the market for biometric solutions may be adversely affected. Even if biometric technologies gain wide market acceptance, our biometric products and services may not adequately address the requirements of the market and may not gain widespread commercial acceptance.

We face intense competition, which could result in lower revenues and higher research and development expenditures and could adversely affect our results of operations.

The events of September 11, 2001 and subsequent regulatory and policy changes in the U.S. and abroad have heightened interest in the use of biometric security solutions, and we expect competition in this field, which is already substantial, to intensify. Competitors are developing and marketing semiconductor ultrasonic and optically based direct contact fingerprint image capture devices, or retinal blood vessel, iris pattern, hand geometry, voice or various types of facial structure solutions. Among these companies are Cognitec Systems Corporation, CrossMatch

Technologies, Imaware Systems, Inc., SAGEM Morpho Inc., NEC Corporation, Cogent, Inc. and Ultra-Scan Corporation. Our products also compete with non-biometric technologies such as certificate authorities and traditional keys, cards, surveillance systems and passwords. Widespread adoption of one or more of these technologies or approaches in the markets we intend to target could significantly reduce the potential market for our systems and products. Some of our competitors have significantly more

28

Table of Contents

resources than we have. Our competitors may introduce products that are more price competitive, have increased performance or functionality or incorporate technological advances that we have not yet developed or implemented. To remain competitive, we must continue to develop, market and sell new and enhanced systems and products at competitive prices, which will require significant research and development expenditures. If we do not develop new and enhanced products or if we are not able to invest adequately in their research and development activities, our business, financial condition and results of operations could be severely and negatively impacted.

Unless we keep pace with changing technologies, we could lose existing customers and fail to win new customers.

In order to compete effectively in the biometrics market, we must continually design, develop and market new and enhanced products. Our future success will depend, in part, upon our ability to address the changing and sophisticated needs of the marketplace. Frequently, technical development programs in the biometric industry require assessments to be made of the future directions of technology and technology markets generally, which are inherently risky and difficult to predict. We may not be able to accurately predict which technologies our customers will support. If we fail to choose correctly among technical directions, or we fail to offer innovative products and services at competitive prices in a timely manner, customers may forego purchases of our products and services and purchase those of our competitors.

Security breaches in systems that we sell or maintain could result in the disclosure of sensitive government information or private personal information that could result in the loss of customers and negative publicity.

Many of the systems we sell manage private personal information and protect information involved in sensitive government functions. The protective security measures that we use in these systems may not prevent security breaches, and failure to prevent security breaches may disrupt our business, damage our reputation, and expose us to litigation and liability. A party who is able to circumvent protective security measures used in these systems could misappropriate sensitive or proprietary information or cause interruptions or otherwise damage our products, services and reputation, and the property and privacy of our customers. If unintended parties obtain sensitive data and information, or create bugs or viruses or otherwise sabotage the functionality of our systems, we may receive negative publicity, incur liability to our customers or lose the confidence of our customers, any of which may cause the termination or modification of our contracts. Further, our insurance coverage may be insufficient to cover losses and liabilities that may result from such events.

In addition, we may be required to expend significant capital and other resources to protect ourselves against the threat of security breaches or to alleviate problems caused by the occurrence of any such breaches. However, protective or remedial measures may not be available at a reasonable price or at all, or may not be entirely effective if commenced.

Our reliance on external suppliers and contract manufacturers may result in disruption of our operations.

The lead-time for ordering certain of products and materials and for building many of our products can be many months. As a result, we must order products and materials based on forecasted demand. If demand for our products lags significantly behind our forecasts, we may purchase more products than we can sell, which can result in increased cash needs and write-downs of obsolete or excess inventory. In addition, if product purchases are delayed, we may lose customers and sales.

We rely on contract manufacturers to produce our hardware products under short term manufacturing arrangements. Although we believe we can find alternative sources of manufacturing our hardware, any disruption of contractual arrangements could result in delaying deliveries or in the loss our sales. We obtain certain hardware and services, as

well as software applications, from a limited group of suppliers. Our reliance on these suppliers involves significant risks, including reduced control over quality and delivery schedules. In particular, we are dependent on a single supplier for all

29

Table of Contents

of the printers and consumables for the U.S. Department of State passport contract and the U. S. Department of Defense common access card contract. Any financial instability of our suppliers could result in our having to find new suppliers. We may experience significant delays in manufacturing and deliveries of our products and services to customers if we lose our sources or if supplies and services delivered from these sources are delayed. As a result, we may be required to incur additional development, manufacturing and other costs to establish alternative sources of supply. It may take several months to locate alternative suppliers, if required, or to re-tool our products to accommodate components from different suppliers. We cannot predict if we will be able to obtain replacement components within the time frames we require at an affordable cost, or at all. Any delays resulting from suppliers failing to deliver components or obtain alternative service providers, products or services on a timely basis, in sufficient quantities and of sufficient quality or any significant increase in our costs of components from existing or alternative suppliers could have a severe negative impact on our business, financial condition and results of operations.

The market for our solutions is still developing and if the biometrics industry adopts standards or a platform different from our platform, then our competitive position would be negatively affected.

The market for identity solutions is still developing. The evolution of this market may result in the development of different technologies and industry standards that are not compatible with our current solutions, products or technologies. Several organizations, such as the International Civil Aviation Organization, sets standards for travel documents that its member states then put into effect, and the National Institute for Standards and Testing, which is part of the U.S. Department of Commerce, set standards for biometrics to be used in identification and documentation. Although we believe that our biometric technologies comply with existing standards for finger, face and iris recognition, these standards may change and any standards adopted could prove disadvantageous to or incompatible with our business model and current or future solutions, products and services.

Our plan to pursue sales in international markets may be limited by risks related to conditions in such markets.

In the year ended December 31, 2007, we derived approximately 7% of our total revenues from international sales and our strategy is to expand our international operations. There is a risk that we may not be able to successfully market, sell and deliver our products in foreign countries.

Risks inherent in marketing, selling and delivering products in foreign and international markets, each of which could have a severe negative impact on our financial results and stock price, include those associated with:

- regional economic or political conditions;
- delays in or absolute prohibitions on exporting products resulting from export restrictions for certain products and technologies;
- loss of, or delays in importing products, services and intellectual property developed abroad, resulting from unstable or fluctuating social, political or governmental conditions;
- fluctuations in foreign currencies and the U.S. dollar;
- loss of revenue, property (including intellectual property) and equipment from expropriation, nationalization, war, insurrection, terrorism, criminal acts and other political and social risks;
- liabilities resulting

from any unauthorized actions of our local resellers or agents under the Foreign Corrupt Practices Act or local anti-corruption statutes;

different tax structures;

taxes and other government fees; and

renegotiations of contracts with foreign governments.

- the overlap of
- risks of increases in
- involuntary

We expect that we will have increased exposure to foreign currency fluctuations. As of December 31, 2007, our accumulated other comprehensive income includes foreign currency

30

Table of Contents

translation adjustments of \$6.4 million. In addition, we have significant Japanese yen denominated transactions with Japanese suppliers of hardware and consumables for the delivery to customers under certain material contracts. Fluctuations in foreign currencies, including our Japanese yen denominated and Canadian dollar denominated transactions could result in unexpected fluctuations to our results of operations, which could be material and adverse.

If we do not successfully expand our direct sales and services organizations and partnering arrangements, we may not be able to increase our sales or support our customers.

We sell substantially all of our services and license substantially all of our products through our direct sales organization. Our future success depends on substantially increasing the size and scope of our direct sales force and partnering arrangements, both domestically and internationally. We will face intense competition for personnel, and we cannot guarantee that we will be able to attract, assimilate or retain additional qualified sales personnel on a timely basis. Moreover, given the large-scale deployment required by some of our customers, we will need to hire and retain a number of highly trained customer service and support personnel. We cannot guarantee that we will be able to increase the size of our customer service and support organization on a timely basis to provide the high quality of support required by our customers. The ability to add additional sales and customer service personnel could result in customer dissatisfaction and loss of customers.

We rely in part upon system integrators original equipment manufacturers, or OEM, and distribution partners to sell our products, technologies and services, and we may be adversely affected if those parties do not actively promote their products or pursue installations that do not use our products, technologies and services.

A portion of our revenue comes from sales to partners including OEMs, systems integrators, distributors and resellers. Some of these relationships have not been formalized in a detailed contract, and may be subject to termination at any time. Even where these relationships are formalized in a detailed contract, the agreements can often be terminated with little or no notice and subject to periodic amendment.

We intend to continue to seek strategic relationships to distribute, license and sell certain of our products. We, however, may not be able to negotiate acceptable relationships in the future and cannot predict whether current or future relationships will be successful.

For example, we are currently involved in a dispute with LG Electronics, Inc. and its subsidiary relating to the termination of such a relationship. As a result of this dispute, LG has alleged the invalidity of Iridian's patents, copyrights and trade secrets. A material adverse ruling against Iridian respecting either the underlying contract claims or enforceability of Iridian's intellectual property rights could materially adversely impact the value of the Company's investment in Iridian and its iris recognition technology. See Item 3. "Legal Proceedings."

If our systems and products are not timely delivered or do not perform as promised, we could experience increased costs, lower margins, liquidated damage payment obligations and reputational harm.

We often provide complex systems that are required to operate in difficult or sensitive circumstances. The development of such complex systems may be subject to delays or failure to meet performance requirements to customer specifications. The negative effects of any delay or failure to deliver to meet performance requirements could be exacerbated if the delay or failure occurs in systems that provide personal security, secure sensitive computer data, authorize significant financial transactions or perform other functions where a security breach could have significant consequences. If a product launch is delayed or is the subject of an availability shortage because of problems with our ability to manufacture or assemble the product successfully on a timely basis, or if a product or

service otherwise fails to meet performance criteria, we may lose revenue opportunities entirely and/or experience delays in revenue recognition associated with a product or service in addition to incurring higher operating expenses during the period required to correct the defects.

There is a risk that for unforeseen reasons we may be required to repair or replace a substantial number of products in use or to reimburse customers for products that fail to work or meet strict

31

Table of Contents

performance criteria. From time to time, in certain critical or complex sale or licensing transactions, we may be compelled to accept liability provisions that vary from our preferred contracting model. There is a risk that in certain contracts and circumstances we may not be successful in adequately minimizing our product and related liabilities or that the protections we negotiate will not ultimately be deemed enforceable. We carry product liability insurance, but existing coverage may not be adequate to cover potential claims. Although we will deploy back-up systems, the failure of our products to perform as promised could result in increased costs, lower margins, liquidated damage payment obligations and harm to our reputation. This could result in contract terminations and have a material adverse effect on our business and financial results.

Failure to maintain the proprietary nature of our technology, intellectual property and manufacturing processes could have a material adverse effect on our business and our ability to compete effectively.

We principally rely upon patent, trademark, copyright, trade secret and contract law to establish and protect our proprietary rights. There is a risk that claims allowed on any patents or trademarks we hold may not be broad enough to protect our technology. In addition, our patents or trademarks may be challenged, invalidated or circumvented and we cannot be certain that the rights granted there under will provide competitive advantages to us. Moreover, any current or future issued or licensed patents, or trademarks, or currently existing or future developed trade secrets or know-how may not afford sufficient protection against competitors with similar technologies or processes, and the possibility exists that certain of our already issued patents or trademarks may infringe upon third party patents or trademarks or be designed around by others. In addition, there is a risk that others may independently develop proprietary technologies and processes, which are the same as, substantially equivalent or superior to ours, or become available in the market at a lower price.

We may be acquired to expend significant resources to monitor and protect our intellectual property rights. We may have to litigate to enforce our patents or trademarks or to determine the scope and validity of other parties' proprietary rights. Litigation could be very costly and divert management's attention. An adverse outcome in any litigation may have a severe negative effect on our financial results and stock price. To determine the priority of inventions, we may have to participate in interference proceedings declared by the United States Patent and Trademark Office or oppositions in foreign patent and trademark offices, which could result in substantial cost and limitations on the scope or validity of our patents or trademarks.

In addition, foreign laws treat the protection of proprietary rights differently from laws in the United States and may not protect our proprietary rights to the same extent as U.S. laws. The failure of foreign laws or judicial systems to adequately protect our proprietary rights or intellectual property, including intellectual property developed on our behalf by foreign contractors or subcontractors may have a material adverse effect on our business, operations, financial results and stock price.

Legal claims regarding infringement by us or our suppliers of third party intellectual property rights could result in substantial costs, diversion of managerial resources and harm to our reputation.

Although we believe that our products and services do not infringe currently existing and validly issued intellectual property rights of others, we might not be able to defend successfully against a third-party infringement claim. A successful infringement claim against us, our customers or our suppliers could subject us to:

- liability
- for damages and litigation costs, including attorneys' fees;
- lawsuits that

prevent us from further use of the intellectual property;

the intellectual property from a third party, which could include significant licensing fees;

non-infringing alternative, which could be costly and delay projects;

clients with respect to losses they incurred as a result of the alleged infringement; and

alternative sources for products supplied to us by third parties, as discussed above in the risk factor regarding their dependence on limited source suppliers.

- having to license
- having to develop a
- having to indemnify
- having to establish

Table of Contents

Our failure to prevail against any third party infringement claim could have a material adverse effect on our business and financial results. Even if we are not found liable in a claim for intellectual property infringement, such a claim could result in substantial costs, diversion of resources and management attention, termination of customer contracts and harm to our reputation.

We may be unable to obtain additional capital required to finance our growth and our acquisition strategy may be adversely affected by unpredictable and unstable market conditions.

Our strategy includes growth of our business through strategic acquisitions. In addition, the installation of our secure credentialing systems requires significant capital expenditures. At December 31, 2007, we had cash and cash equivalents of \$8.2 million and availability under our line of credit of \$57.3 million. While we believe we have adequate capital resources to meet current working capital and capital expenditure requirements and have been successful in the past in obtaining financing for working capital, capital expenditures, and acquisitions, we expect to have increased capital needs as we continue to expand our business. In addition, our acquisition strategy may be adversely affected by unpredictable and unstable market conditions. Particularly during periods of adverse economic conditions or during a tightening of global credit markets, we may be unsuccessful in raising additional financing or we may have difficulty in obtaining financing at attractive rates or on terms that are not excessively dilutive to existing stockholders. Failure to secure additional financing in a timely manner and on favorable terms could have a material adverse effect on our growth strategy, financial performance and stock price and could require us to delay or abandon our expansion plans.

We are dependent on a small number of individuals, and if we lose key personnel upon whom we are dependent, our business will be adversely affected.

Much of our future success depends on the continued service and availability of our senior management, including our Chairman of the Board, President and Chief Executive Officer, Robert V. LaPenta, and other members of our executive team. These individuals have acquired specialized knowledge and skills with regards to advanced technology identity solutions. The loss of any of these individuals could severely harm our business. Our business is also highly dependent on our ability to retain, hire and motivate talented highly skilled personnel. Experienced personnel in the advanced technology identity solutions industry are in high demand and competition for their talents are intense. If we are unable to successfully attract, retain and motivate key personnel, our business may be severely harmed.

If we fail to recruit and retain skilled employees or employees with the necessary security clearances, we might not be able to perform under our government services contracts or win new business.

To be competitive, we must have employees who have advanced information technology and technical services skills and who work well with our customers in a government or defense-related environment. Often, these employees must have some of the highest security clearances in the United States. These employees are in great demand and are likely to remain a limited resource in the foreseeable future. If we are unable to recruit and retain a sufficient number of these employees, our ability to maintain and grow our business could be negatively impacted. In addition, some of our government services contracts contain provisions requiring us to commit to staff a program with certain personnel the customer considers key to our successful performance under the contract. In the event we are unable to provide these key personnel or acceptable substitutions, the customer may terminate the contract, and we may not be able to recover certain incurred costs.

Certain of our stockholders have significant relationships with us, which could result in it taking actions that are not supported by unaffiliated stockholders.

In connection with the Aston investment, Aston became the largest stockholder of L-1, owning approximately 10.1% of our outstanding common stock. In addition, Lau Technologies, or (“Lau”) beneficially owns approximately 2.8% of our outstanding common stock. As a result, Aston (together with its affiliate, L-1 Investment Partners LLC) and Lau have an influence on matters requiring

33

Table of Contents

approval by our stockholders, including the election of directors and most corporate actions, such as mergers and acquisitions. In addition, we have significant relationships with each of L-1 Investment Partners LLC, Aston and Lau including:

- Mr. Robert V. LaPenta, the founder and Chief Executive Officer of L-1 Investments Partners LLC, is Chairman of our board of directors and Chief Executive Officer and President;

- Mr. James DePalma, Mr. Joseph Paresi and Ms. Doni Fordyce who are affiliates of L-1 Investment Partners LLC and Aston, serve as the Executive Vice President and Chief Financial Officer, Executive Vice President and Chief Marketing and Sales Officer, and Executive Vice President and of Corporate Communications, respectively;

- we acquired intellectual property, contracts and distribution channels through a transaction with Lau in January 2002 under which we agreed to pay Lau a 3.1% royalty on certain of our face recognition revenues through June 30, 2014, up to a maximum of \$27.5 million;

- in connection with the above transaction with Lau, we entered into consulting agreements with Ms. Joanna Lau, the President of Lau, and her spouse Mr. Denis K. Berube, the Chief Operating Officer of Lau who also serves as a director on our board of directors, under which we will pay each of Ms. Lau and Mr. Berube \$0.1 million per year through the earlier of January 10, 2012 or the commencement of the consultants' full-time employment elsewhere. Mr. Berube and Ms. Lau own a majority of Lau's stock.

The concentration of large percentages of ownership in any single stockholder, or in any series of single stockholders, may delay or prevent change in control of the Company. Additionally, the sale of a significant number of our shares in the open market by single stockholders or otherwise could adversely affect our stock price.

Risks Related to Our Acquisition Strategy

Integration of recently acquired businesses may be difficult to achieve and will consume significant financial and managerial resources, which may adversely affect operations.

Our operating philosophy is to let acquired businesses operate in autonomous manner subject to corporate oversight but integrating and rationalizing duplicative functions to achieve revenue and cost synergies. We may encounter substantial difficulties, costs and delays in integrating the operations recently acquired and future acquisitions such as:

- exposure to unknown liabilities of acquired companies or assets;

- higher than anticipated acquisition costs and expenses;

- assumption of ongoing litigation matters that may be highly complex and involve significant time, cost and expense (such as the dispute with LG assumed with in connection with our acquisition of Iridian and described under "Item 3 Legal Proceedings");

- potential conflicts between business cultures;

- adverse changes in business focus perceived by third-party constituencies;

ongoing business;
in distribution, marketing or other important relationships;
of management resources;
our financial and strategic position by the successful incorporation of acquired technology;
potential of acquired technologies, complete product development, or properly obtain or secure appropriate protection
of intellectual property rights; and
employees and/or the diversion of management's attention from other ongoing business concerns.

- disruption of our
- potential conflicts
- potential constraints
- failure to maximize
- failure to realize the
- loss of key

Table of Contents

The geographic distance between the companies and their respective offices and operations increases the risk that the integration will not be completed successfully or in a timely and cost-effective manner. We may not be successful in overcoming these risks or any other problems encountered in connection with the integration of the companies. The simultaneous integration of these acquisitions may place additional strain on our resources and increase the risk that our business may be adversely affected by the disruption caused by the acquisitions. Our strategy contemplates acquiring additional businesses, the integration of which may consume significant financial and managerial resources, and could have a severe negative impact on our business, financial condition and results of operations.

Our acquisitions could result in future impairment charges and other charges which could adversely affect our results of operations.

At December 31, 2007, goodwill and other intangible assets are \$1,054.3 million and \$184.2 million, respectively. Because goodwill represents a residual after the purchase price is allocated to the fair value of acquired assets and liabilities, it is difficult to quantify the factors that contribute to the recorded amounts. Nevertheless, management believes that the following factors have contributed to the amount recorded:

- technological development capabilities and intellectual capital;
- expected significant growth in revenues and profits from the expanding market in identity solutions; and
- expected synergies resulting from providing multi modal product offerings to existing customer base and to new customers of the combined company.

The recorded amounts at the purchase date for goodwill and other intangible assets are estimates at a point in time and are based on valuations and other analyses of fair value that require significant estimates and assumptions about future events, including but not limited to projections of revenues, market growth, demand, technological developments, political developments, government policies, among other factors, which are derived from information obtained from independent sources, as well as the management of the acquired businesses and our business plans for the acquired businesses or intellectual property. If estimates and assumptions used to initially record goodwill and intangible assets do not materialize, or unanticipated adverse developments or events occur, ongoing reviews of the carrying amounts of such goodwill and intangible assets may result in impairments which will require us to record a charge in the period in which such an impairment is identified, and could have a severe negative impact on its business and financial statements. Subsequent to December 31, 2007, our stock price declined by approximately 30%. If the price remains at the current level for a sustained period of time, we may be required to assess the carrying amounts of goodwill and intangible assets of our reporting units before our scheduled annual impairment test. Our estimated enterprise value at February 26, 2008 exceeds the overall carrying amounts of our reporting units.

If we do not achieve the expected benefits of the acquisitions we have made, the price of our common stock could decline.

We expect that the acquisitions that we consummated in 2006 and 2007, as well as the acquisitions that we have made previously will enhance our leadership in the identity solutions industry through the combination of their respective technologies. However, the combination of such technologies might not meet the demands of the marketplace. If our technologies fail to meet such demand, customer acceptance of our biometric products could decline, which would have an adverse effect on our results of operations and financial condition. Further, we expect that the additions to our solutions offerings will extend our reach into our current markets and provide a critical component to our

comprehensive offering for new markets in need of identity solutions. However, there can be no assurance that our current customers or customers in new markets will be receptive to these additional offerings. Further, we might not be able to market successfully our products and services to the customers of the companies we acquired. If our solutions offerings and services fail to meet the

35

Table of Contents

demands of this marketplace, our results of operations and financial condition could be adversely affected. There is also a risk that we will not achieve the anticipated benefits of the acquisitions as rapidly as, or to the extent, anticipated by financial or industry analysts, or that such analysts will not perceive the same benefits to the acquisitions as they do. If these risks materialize, our stock price could be adversely affected.

Item 1B.

Unresolved Staff Comments

None

Item 2.

Properties

We do not own any properties. The following describes our most significant leasing arrangements.

Our corporate headquarters comprises approximately 16,600 square feet of space in facilities located in Stamford, Connecticut. We sublease space from L-1 Investment Partners LLC. The sublease terminates on the earlier of the date that the Company's Chairman and Chief Executive Officer ceases employment with the Company or March 2010. We use this property for corporate, administrative, customer support and other general business needs. We also lease the following facilities:

- 39,200 square feet of space in Billerica, MA which is under a lease that expires in 2008. The space houses the headquarters and operations of our Viisage division. Also the division leases 5,100 square feet of space in Harrisburg, PA and the lease expires in 2011.
- 15,000 square feet of space in Springfield, IL which is under a lease that expires in 2010. The space houses certain operating and administrative staff of IBT.
- 59,000 square feet of space in Bloomington, MN which expires in 2014. The space houses the headquarters and operations of our Identix division.
- 18,000 square feet in Jersey City, NJ under a lease that expires in April 2017. The space houses our research and development operations.
- 15,700 square feet in Reston, VA under a lease that expires in March 2012. The space houses the headquarters and operations of the SpecTal division.
- 12,000 square feet in Fairfax, VA under a lease that expires in December 2009. We have vacated this space and are seeking to sublease it.
- 12,500 square feet of space in facilities located in Bochum, Germany. The term of this lease is indefinite, but the lease can be terminated on six months' notice. This space is used for research and development and sales operations.
- 19,700 square feet of space in Arlington, Virginia. The term of this lease runs through December 2012. We use this property for our federal sales and marketing operations.
- 6,700 square feet of space in Nashville, Tennessee, which is used for the headquarters and operations of IBT. The term of this lease runs through July 2009. In addition, the division has leased 1,000 square feet in Long Beach, CA for IBT operations under

a lease that expires in 2009.

of space in Martinez, California, which houses the headquarters and operations of SecuriMetrics and Iridian. The term of this lease runs through February 2011.

Oakville, Ontario, Canada, on a month to month basis which houses the headquarters of ComnetiX. We also lease approximately 6,000 square feet in Carrollton, Georgia, on a month to month basis, which houses the U.S. operations of ComnetiX.

Columbia, MD which houses the headquarters and operations of ACI. The term of the lease runs through December 2012. In addition, the division has leased 3,000 square feet in Washington, DC, 2,500 square feet in Warner Robins, GA, 1,500 square feet in Melbourne, FL and 1,000 in McLean, VA.

in Chantilly, VA, which houses our McClendon headquarters and operations. The term of this lease runs through May 2010.

36

Table of Contents

While we believe that these facilities are adequate to meet our immediate needs, it may become necessary to secure additional space in the future to accommodate any future growth. We believe that such additional space will be available as needed in the future on commercially reasonable terms.

Item 3.

Legal Proceedings

In January 2004, LG Electronics USA, Inc. and LG Electronics, Inc. (a Korean corporation) (“LG”) filed a lawsuit against Iridian Technologies, Inc., a wholly owned subsidiary of the Company, in federal court in New Jersey seeking to cancel Iridian’s federal trademark registration for its IrisAccess trademark, and alleging that Iridian had made false statements by announcing that it had discontinued its IrisAccess line of products. At the time LG filed this lawsuit, the parties had been engaged in an ongoing negotiation regarding Iridian’s introduction of new standard pricing for its licenses. LG contended that Iridian was not entitled to impose its new standard “per user” pricing on LG pursuant to the terms of the parties’ 2000 Amended and Restated Development, Distribution and Supply agreement (the “License Agreement”). In August 2004, LG filed a demand for arbitration before the American Arbitration Association, seeking a finding that its fee for using Iridian’s iris recognition technology remained at the original “per unit” pricing structure under the License Agreement. Shortly thereafter, Iridian terminated the License Agreement due to LG’s failure to pay royalties as required under Iridian’s new standard pricing. In response, LG filed another lawsuit in New Jersey federal court, asking the court to enter a finding that Iridian’s termination of the License Agreement was improper and that LG’s continued use of Iridian’s technology did not infringe upon Iridian’s patent rights. The issues in all three cases have since been consolidated into one action pending in New Jersey federal court, and are being litigated pursuant to a series of amended complaints filed by LG. Iridian vigorously denies all of LG’s claims and is counterclaiming for LG’s breach of contract, infringement of Iridian’s patents and copyrights, and misappropriation of Iridian’s trade secrets. LG has replied to Iridian’s counterclaims and has asserted defenses that include, among other things, the alleged invalidity or unenforceability of Iridian’s patents, copyrights and trade secrets. Late in 2006, the court allowed LG to further amend its complaint to add allegations of antitrust violations by Iridian and on July 5, 2007, the court allowed LG to amend its complaint again to assert claims against L-1 and SecuriMetrics as defendants. Iridian has requested to assert additional counterclaims against LG and such request remains pending while the Court conducts mediation with all parties in an effort to reach settlement terms. Iridian believes that it has strong defenses to all of LG’s claims and a strong basis to pursue all of Iridian’s counterclaims, and intends to vigorously defend against LG’s claims and pursue its own counterclaims if a settlement is not reached. At this time, it is not possible to predict with certainty the outcome of this litigation or the terms or probability of any settlement. A material adverse ruling against Iridian respecting either the underlying contract claims or enforceability of Iridian’s intellectual property rights could materially adversely impact the value of the Company’s investment in Iridian and its iris recognition technology. Pre-trial proceedings in the consolidated action are ongoing and no trial date has yet been set.

In March and April 2005, eight putative class action lawsuits were filed in the United States District Court for the District of Massachusetts against L-1, Mr. Bernard C. Bailey, Mr. William K. Aulet (the Company’s former Chief Financial Officer) and Mr. Denis K. Berube and other members of the Board of Directors of Viisage Technology, Inc. (“Viisage”). These lawsuits have been consolidated into one action under one case name: In re: Viisage Technology Securities Litigation, Civil Action No. 05-10438-MLW (the “Securities Litigation”). The so-called Turnberry Group has been designated as lead plaintiff and its counsel has been designated as lead counsel. The amended consolidated complaint that was filed in February 2006 alleges violations of the federal securities laws by Viisage (now named L-1 Identity Solutions, Inc.) and certain officers and directors arising out of purported misstatements and omissions in Viisage’s SEC filings related to certain litigation involving the Georgia drivers’ license contract and related to the Viisage’s reported material weaknesses in internal controls over financial reporting, which allegedly artificially inflated the price of the Company’s stock during the period May 12, 2004 through March 2, 2005. In April 2006, the

Company filed a motion to dismiss this case. In February 2007, the judge dismissed all claims related to the Georgia drivers' license contract and permitted the case to proceed on claims associated with purported internal control weaknesses over financial reporting. On July 19, 2007, the Company and

37

Table of Contents

counsel for the lead plaintiff executed a Stipulation of Settlement settling the Securities Litigation. Under the terms of the Stipulation of Settlement, the defendants were to make a payment to the plaintiff class in the amount of \$2.3 million. That payment was funded by the Company's directors and officers' insurance carrier. After notice to the class and a hearing, the Court issued an order approving the settlement on November 16, 2007. No appeal from that order was filed, and it has become final.

In April 2005, two purported shareholder derivative actions also were filed against directors, naming Viisage as a nominal defendant. The suits claim that these directors breached their fiduciary duties to Viisage's shareholders and to Viisage generally in connection with the same set of circumstances alleged in the class action lawsuit. The complaints are derivative in nature and do not seek relief from the Company. One of these actions was filed in Massachusetts Superior Court and the other was filed in the United States District Court for the District of Massachusetts. In July 2005, the state court action was dismissed with prejudice at the plaintiff's request. An amended complaint in the federal court derivative action was filed in July 2006 in which the plaintiff added allegations regarding disclosures by Viisage's representatives that generally appear to be intended to support her contention that she was excused from making a demand on the board of directors before filing a derivative complaint. The Company filed a motion to dismiss the amended complaint. After briefing and oral argument, the Court issued a memorandum and order allowing the motion and dismissing the amended complaint on August 23, 2007. The plaintiff filed a notice of appeal from this order on September 24, 2007. The Company anticipates that briefing and argument before the First Circuit Court of Appeals will be complete before the end of the 2008. The Company believes that derivative actions are without merit and that the District Court's decision will be affirmed.

Item 4

Submission of Matters to a Vote of Security Holders

None.

38

Table of Contents

PART II

Item 5.

Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

Market for Our Common Stock

Our common stock is traded on the New York Stock Exchange under the symbol “ID.” Prior to August 30, 2006 our common stock traded on the NASDAQ National Market under the symbol “VISG.” As of February 22, 2008, there were 1,626 holders of record of our common stock.

The quarterly high and low sales prices, as reported by the New York Stock Exchange or NASDAQ, as applicable, of our common stock during 2007 and 2006 were as follows:

2007	2006	Quarter	High	Low	High	Low	First Quarter	\$ 17.12	\$ 14.15	\$ 19.25	\$ 15.73	Second
Quarter	\$ 21.87	\$ 16.31	\$ 17.65	\$ 12.99	Third Quarter	\$ 20.95	\$ 13.75	\$ 17.33	\$ 13.03	Fourth		Quarter
Quarter	\$ 19.54	\$ 16.50	\$ 17.25	\$ 12.40								

Dividend Policy

We paid no dividends in 2007 or 2006. We presently intend to retain our cash for use in the operation and expansion of our business and, therefore, do not anticipate paying any cash dividends in the foreseeable future. In addition, we are prohibited from paying dividends pursuant to our revolving credit agreement.

Recent Sales of Unregistered Securities

We did not sell any unregistered securities during the fourth quarter of 2007.

Repurchases of Common Stock

We did not repurchase any shares of our common stock during the fourth quarter of 2007.

Table of Contents

Stock Performance Chart

The following performance chart assumes an investment of \$100 on December 31, 2002 and compares the change to December 31, 2007 in the market price for our common stock with the Russell 2000 Index, the NASDAQ Composite Index, and a peer group identified by the Company (the “Selected Peer Group Index”). The Selected Peer Group Index was selected to include publicly-traded companies engaging in one or more of the Company’s lines of business.

The Selected Peer Group Index is weighted according to the respective issuer’s stock market capitalization and is comprised of the following companies: Cogent Inc., ActivIdentity Corporation, DigiMarc Corporation, LaserCard Corporation, Bioscrypt Inc., ImageWare Systems, Inc. and Saflink Corporation.

The comparisons in the graph below are based on historical data and are not intended to forecast the possible future performance of our common stock.

Stock Performance Chart

40

Table of Contents

Supplemental Stock Performance Chart

The following chart supplements the stock performance chart presented above to show the stock performance from October 5, 2005, the day prior to the date that Aston Capital Partners LP announced its investment in L-1, through December 31, 2007 since during this period the Company underwent significant changes in operations and capital structure, including the issuance of \$100 million of common stock to Aston, the merger with Identix and acquisitions of IBT, SecuriMetrics, Iridian, SpecTal, ComentiX, ACI and McClendon, as well as significant changes in the board of directors and management.

Supplemental Chart

Item 6.

Selected Financial Data

The financial data set forth below should be read in conjunction with “Management’s Discussion and Analysis of Financial Condition and Results of Operations” and our audited consolidated financial statements as of December 31, 2007 and 2006 and for each of the three years in the period ended December 31, 2007 and the related notes included elsewhere in this report on Form 10-K. The historical results of operations are not necessarily indicative of future results.

41

Table of Contents

		Years Ended December 31,		2007(1)	2006(1)	2005	2004	2003	(in thousands, except per share data)		
Statement of Operations Data:						Revenues	\$ 389,507	\$ 164,386	\$ 66,224	\$	
67,466	\$ 37,371	Cost of revenues		268,431	113,529	47,568	48,804	27,844	Gross profit		
121,076	50,857	18,656	18,662	9,527	Operating expenses:		Sales and marketing				
27,719	14,430	7,832	6,925	5,282	Research and development		18,482	11,589	4,618		
3,837	3,650	General and administrative		62,279	29,953	12,068	9,779	5,110	Asset impairments and merger related expenses		
401	681	153	—	5,000	22,767	—	2,000	—	Amortization of intangible assets		
401	681	153	—	Total operating expenses		115,999	79,140	25,199	22,694	14,042	
Operating income (loss)		5,077	(28,283)	(6,543)	(4,032)	(4,515)	Interest income		407	1,770	362
162	99	Interest expense		(11,311)	(1,598)	(159)	(1,933)	(1,068)	Other (expense) income, net		
(508)	(122)	369	(235)	18	Loss before income taxes and cumulative effect of change in accounting principle		(6,335)	(28,233)	(5,971)	(6,038)	(5,466)
(2,804)	(1,382)	(959)	(63)	Income (loss) before cumulative effect of change in accounting principle		17,666	(31,037)	(7,353)	(6,997)	—	
—	—	—	(12,131)	Net income (loss)		\$ 17,666	\$ (31,037)	\$ (7,353)	\$ (6,997)	\$ (17,660)	
Basic income (loss) per share before cumulative effect of change in accounting principle		\$ 0.25	\$ (0.71)	\$ (0.37)	\$ (0.45)	\$ (0.64)	Diluted income (loss) per share before cumulative effect of change in accounting principle		\$ 0.24	\$ (0.71)	\$ (0.37)
\$ (0.45)	\$ (0.64)	Diluted income (loss) per share before cumulative effect of change in accounting principle		\$ 0.24	\$ (0.71)	\$ (0.37)	\$ (0.45)	\$ (0.64)	Cumulative effect of change in accounting principle per share		
—	—	—	—	Net income (loss) per share:		Basic		\$ 0.25	\$ (0.71)	\$ (0.37)	
)	\$ (0.45)	\$ (2.06)	Diluted	\$ 0.24	\$ (0.71)	\$ (0.37)	\$ (0.45)	\$ (2.06)	Weighted average common shares outstanding:		
Diluted	72,385	43,823	19,630	15,466	8,578	Balance Sheet Data:		Current			
assets, net of current liabilities		\$ 40,869	\$ 11,658	\$ 77,482	\$ 15,233	\$ 5,887	Total assets		\$ 1,445,645		
\$ 1,227,225	\$ 294,108	\$ 175,629	\$ 54,480	Long-term debt		\$ 259,000	\$ 80,000	\$ 215	\$ 149		
\$ 8,147	Shareholders' equity		\$ 1,084,717	\$ 1,067,085	\$ 274,660	\$ 154,790	\$ 34,008				

(1) The

results reflect the adoption of SFAS No. 123(R) on January 1, 2006.

Item 7. Management's

Discussion and Analysis of Financial Condition and Results of Operations

Introduction

The following discussion and analysis should be read in conjunction with our consolidated financial statements and the accompanying notes thereto included in "Item 8. Financial Statements and Supplementary Data" of this report.

Table of Contents

Business Overview

L-1 Identity Solutions, Inc. provides identity protection solutions that enable governments, law enforcement agencies and businesses to enhance security, reduce identity theft, and protect personal privacy. Our solutions are specifically designed for the identification of people and include secure credentialing, biometrics, automated document authentication, real-time identity databases, automated testing of identity and identity information, and biometrically-enabled background checks, as well as systems design, development, integration and support services. These identity solutions enable our customers to manage the entire life cycle of an individual's identity for a variety of applications including civil identification, criminal identification, border management, anti-terrorism, and security. The Company also provides comprehensive consulting, training, security, technology development and information technology solutions to the U.S. intelligence community.

The Company offers solutions that include products and related services, comprising of hardware, components, consumables and software, as well as maintenance, consulting and training services. In addition, the company provides stand alone enrollment services and government consulting, training, security technology development and information technology services. A customer, depending on its 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.

The market for identity protection solutions has continued to develop at a rapid pace. In particular, 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 to meet our customer needs, 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 evaluate our business primarily through financial metrics such as revenues, operating income (loss) and earnings before interest-net, income taxes, depreciation and amortization, asset impairments and in-process research and development charges, and stock-based compensation expense ("Adjusted EBITDA"), and free cash flow.

Our revenues increased to \$389.5 million for the year ended December 31, 2007 from \$164.4 million for the year ended December 31, 2006. Our net income for the year was \$17.7 million compared to a \$31.0 million loss in 2006. The 2007 and 2006 results include asset impairments and merger related expenses of approximately \$5.0 million and \$22.8 million, respectively. The 2007 results include an income tax benefit of \$21.8 million resulting from the reduction of a portion of the deferred tax asset valuation allowance.

Sources of Revenues

Our Secure Credentialing Division, formerly known as "Viisage," which prior to December 15, 2005 comprised our sole business, generates revenues from the sales of biometric solutions consisting of bundled proprietary software with commercial off-the-shelf equipment and related maintenance and services, the sale of secure printing solutions and related consumables, and the design, customization and installation of secure credential issuance systems which generate revenues as the credentials are issued by the customer. The division also generates revenues from solutions using biometric technologies of other divisions. The division is included in our Identity Solutions segment.

Our Identix Incorporated ("Identix") division, also included in our Identity Solutions segment, generates revenues from the sale of biometric solutions incorporating fingerprint, facial, skin and iris biometrics and system components necessary for the biometric capture and knowledge discovery. Identix offerings include Live Scan and mobile systems

and services for biometric capture and identification, systems and biometric solutions that include modules and software for biometric matching and verification. Revenues are generated by sales of hardware, software and maintenance and other services.

Our SecuriMetrics, Inc. (“SecuriMetrics”)/Iridian Technologies, Inc. (“Iridian”) division, included in our Identity Solutions segment, generates revenues through the development, customization and

43

Table of Contents

sale of biometrics solutions using iris technology which typically consists of proprietary multi-biometric capture devices bundled together with our proprietary software and other biometric technologies as well as sales of licenses and software.

Our Integrated Biometric Technology, Inc. (“IBT”)/Identix Identification Services, Inc. (“IIS”) division, included in our Services segment, generates revenues through the sales of enrollment and background screening products and services.

Our SpecTal, LLC (“SpecTal”) division, included in our Services segment, provides comprehensive security consulting services to U.S. government intelligence agencies.

Our McClendon LLC (“McClendon”) division, included in our Services segment, provides technical and professional services to the U.S. intelligence and military communities.

Our Advanced Concepts, Inc. (“ACI”) division, included in our Services segment, provides information technology and network security solutions, and system engineering and development services for the U.S. intelligence and military communities.

Our ComnetiX Inc. (“ComnetiX”) division, which was acquired on February 21, 2007, provides fingerprinting biometric authentication and identification solutions and enrollment services. The division is included in our Services segment. In 2008, the company expects to separate the biometric authentication and identification business and integrate it in the Identix division.

We market our solutions and services primarily to U.S. and foreign, federal, state and local government agencies and law enforcement agencies. We also are working to expand the use of our solutions in commercial markets, particularly financial services, transportation and healthcare. In a typical contract with a government entity for an identity solution, we design the system, supply and install equipment and software and integrate the solution within the entity’s existing network infrastructure and provide maintenance services. These contracts may be structured as fixed price contracts with payments made upon completion of agreed milestones or deliveries and with each milestone or delivery typically having a value specified in the contract. Alternatively, these contracts may be paid at a fixed price per credential issued as is typical in the drivers’ license market, per fingerprint delivered in the case of our fingerprinting services or on a time and material and fixed price level of effort basis for our government services.

Our growth in revenues is due principally to acquisitions we consummated, as well as increased demand for our identity solutions related to heightened emphasis on security, secure credentials, document authentication and biometrics. We anticipate that the U.S. government agencies will continue to be major customers for the foreseeable future. We also anticipate steadily increasing funding for major government programs. Any delay or other changes in the rollout of these programs could cause our revenues to fall short of expectations. We also expect to experience increased demand from a number of other government entities as they deploy identity solutions, particularly document authentication, at points of entry and exit, including borders, seaports and airports and in connection with national identification programs. Notwithstanding our expectations regarding demand for these solutions, the quantity and timing of orders from both U.S. and foreign government entities depends on a number of factors outside of our control, such as the level and timing of budget appropriations.

Table of Contents

Acquisitions

We have pursued strategic acquisitions to complement and expand our existing solutions and services. Our acquisitions since January 1, 2006 include:

- Our July 2007 acquisitions of McClendon and ACI, which provide technical, network security and professional services to the U.S. intelligence community;
- Our February 2007 acquisition of ComnetiX, which creates an important presence for us in the Canadian market by adding a complementary base of customers to our portfolio, particularly within the law enforcement community;
- Our October 2006 acquisition of SpecTal, which provides comprehensive consulting and security solutions, specializing in government consulting, training and technology development;
- Our August 2006 merger with Identix, whose multi-biometric technology provides a broad range of fingerprint and facial recognition technology offerings, which we believe will expand and better serve our markets at all our divisions;
- Our August 2006 acquisition of Iridian, which holds the leading iris recognition technology in the industry; and
- Our February 2006 acquisition of SecuriMetrics, a provider of the world's only full-function handheld iris recognition and multi-modal biometric devices, enabling us to now offer multiple and multi-modal biometric capabilities that include finger, face and iris technologies.

The acquisitions have resulted in the consolidation of certain marketing resources, facilities and corporate functions of the separate entities in Stamford, Connecticut, and are expected to have a continuing material effect on our operations resulting from, but not limited to:

- Expected synergies resulting from providing a comprehensive product line to current and future customers.
- Expected future growth in revenues and profits from expanded markets for identity solutions.
- Enhancement of technical capabilities resulting from combining the intellectual capital of the combined entities.
- Rationalization of technology costs and research and development activities.
- Realignment of business divisions to complement each division's unique capabilities and rationalizing costs.
- Leveraging the Company's infrastructure to achieve higher revenues and profitability.

Table of Contents

Reportable segments and geographic information

Prior to December 15, 2005, we operated in a single reportable segment, the Identity Solutions segment, and starting with our 2006 year, we changed the reporting of our segments to be aligned with our market opportunities and how we manage our various businesses. We currently operate in two reportable segments, the Identity Solutions segment and the Services segment. We measure segment performance based on revenues, operating income (loss) and Adjusted EBITDA and free cash flow. Operating results by segment for the three years ended December 31, 2007 follow (in thousands):

						Year						
Ended December 31,	2007	2006	2005	Identity Solutions:	Revenues	\$ 202,594	\$ 117,418					
\$ 65,603	Gross Profit	74,112	41,544	18,558	Operating (Loss)	(477)	(29,210)	(6,558)	Adjusted			
EBITDA	44,206	16,292	6,498	Depreciation and Amortization Expense	32,513	21,115	12,357					
Services:				Revenues	186,913	46,968	621	Gross Profit	46,964	9,313	98	Operating
Income	5,554	927	15	Adjusted EBITDA	15,890	4,126	91	Depreciation and Amortization				
Expense	6,724	2,245	76	Consolidated:				Revenues	389,507	164,386	66,224	Gross
Profit	121,076	50,857	18,656	Operating Income (Loss)	5,077	(28,283)	(6,543)	Adjusted				
EBITDA	60,096	20,418	6,589	Depreciation and Amortization Expense	39,237	23,360	12,433					

In 2007 and 2006, the Identity Solutions segment includes asset impairments and merger related costs of \$5.0 million and \$22.8 million, respectively.

Revenue by market comprises the following for the years ended December 31, 2007, 2006 and 2005 (in thousands):

						2007			
2006	2005	State and Local	\$ 109,462	\$ 69,532	\$ 37,683	Federal	269,685	89,640	25,300
		Commercial/Emerging Markets	10,360	5,214	3,241	\$ 389,507	\$ 164,386	\$ 66,224	

Revenues are attributed to each region based on the location of the customer. The following is a summary of revenues by geographic region for the years ended December 31, 2007, 2006 and 2005 (in thousands):

						2007		
2006	2005	Revenue	United States	\$ 360,551	\$ 149,792	\$ 60,267	Rest of World	28,956
14,594	5,957	\$ 389,507	\$ 164,386	\$ 66,224				

Table of Contents

We use Adjusted EBITDA as a non-GAAP financial performance measurement for segments. Adjusted EBITDA is calculated by adding back to net income (loss): interest-net, income taxes, depreciation and amortization, intangible asset impairments, in-process research and development charges, and stock-based compensation expense. Adjusted EBITDA is provided to investors to supplement the results of operations reported in accordance with GAAP. Management believes Adjusted EBITDA is useful to help investors analyze the operating trends of the business before and after the adoption of SFAS No.123 (R) and to assess the relative underlying performance of businesses with different capital and tax structures. Management believes that Adjusted EBITDA provides an additional tool for investors to use in comparing our financial results with other companies in the industry, many of which also use Adjusted EBITDA in their communications to investors. By excluding non-cash charges such as amortization and depreciation, stock-based compensation expense, intangible asset impairments and in-process research and development charges, as well as non-operating charges for interest-net and income taxes, investors can evaluate our operations and can compare our results on a more consistent basis to the results of other companies in the industry. Management also uses Adjusted EBITDA to evaluate potential acquisitions, establish internal budgets and goals, and evaluate performance of our business units and management.

We consider Adjusted EBITDA to be an important indicator of our operational strength and performance of our business and a useful measure of our historical and prospective operating trends. However, there are significant limitations to the use of Adjusted EBITDA since it excludes interest income and expense and income taxes, all of which impact our profitability as well as depreciation and amortization related to the use of long-term assets which benefit multiple periods. We believe that these limitations are compensated for by providing Adjusted EBITDA only with GAAP performance measures and clearly identifying the difference between the two measures. Consequently, Adjusted EBITDA should not be considered in isolation or as a substitute for net income (loss), or operating income (loss) presented in accordance with GAAP. Adjusted EBITDA as defined by the Company may not be comparable with similarly named measures provided by other entities.

A reconciliation of GAAP net income (loss) to Adjusted EBITDA is as follows (in thousands):

	Years
Ended December 31, 2007	