Open the Front Door: There's a New World Outside

The Revolutionary Impact of Networked Applications and Infrastructure White Paper
The A&D and manufacturing market has become more dynamic than ever before. Because of the pace of change and progress, organizations are becoming increasingly reliant on their suppliers to help design, source, and manufacturer products in a more integrated fashion than ever before. Traditional technology applications such as ERP were originally designed to work within the four walls and do not provide the situational awareness required to help companies manage up and down their supply network in an external world—to work with suppliers as true partners, rather than just vendors. To operate effectively in this new environment, companies need to deploy a network approach to managing business processes and technology. In doing so, they must also understand the security and identity assurance requirements necessary to enable a safe foundation for visibility, collaboration, and management outside of the four walls. This whitepaper investigates these areas in more detail, while also providing a step-by-step assessment and guide to help A&D and manufacturers maximize the potential of networked applications and infrastructure.

SETTING THE STAGE: THE EVOLUTION OF THE A&D BUSINESS ENVIRONMENT

Since man first ventured into the skies, the fundamental structure of the aerospace and defense (A&D) industry remained relatively turbulent free for nearly a century. But in recent decades, revolutionary market advances and industry volatility fundamentally impacted the structure of the A&D and manufacturing markets, changing an otherwise steady flight path. Consider how in the year following the tragic events of 9/11, Boeing’s deliveries decreased 28%. Yet between 2003 and 2005, orders for the US aerospace giant rebounded thanks to a new surge in market demand, fueled by significant growth in China and other global regions. This example shows how in today’s market, manufacturers at all levels within the supply chain are expected to respond to demand changes in shorter and shorter time periods. And they must deliver increasingly complex platforms faster and more economically on a global basis, while serving customers in new and creative ways. For example, new business models such as power-by-the-hour (PBTH) and performance based logistics (PBL) are beginning to fundamentally change the basis of compensation and reward in the A&D industry. For example, PBL, which can be defined simply as buying performance, not transactional goods or services, is reshaping the defense acquisition game by changing the sourcing focus to buying results, not inventory, parts, or platforms.

The sum of these changes is making organizations of all sizes reconsider the nature of their relationship with suppliers and partners throughout the value chain. The strategic focus within the supply chain is shifting from internal process management and cost reduction to external collaboration, flexibility, and risk management (including continuity of supply). This fundamental shift is throwing open the front door, exposing a new world of possibilities outside of the four walls of the enterprise. In this world, suppliers are taking an increased role in everything from product design to sourcing to supply chain execution. Indeed, are becoming invaluable as a virtual “network” extension of an organization’s internal capabilities. For nearly all participants, this new net-centric approach is revolutionizing the A&D and manufacturing supply chain. But to operate in this external environment, the industry has to build new levels of visibility and interoperability into their extended operations. For many companies, this flurry of change quickly exposed the limitations of their current systems and capabilities in an environment where suppliers shoulder additional responsibilities. Traditional internal systems of record (i.e., ERP and MRP) and business application environments within the four walls of an organization were designed to manage processes and information within the enterprise, not among a network of key partners.

OVERCOMING THE LIMITATIONS OF INTERNAL ENVIRONMENTS

In a traditional internal systems environment, once an application is deployed, the fundamental architecture allows employees of that enterprise to access, input, or modify information in a secure manner. Much like concrete, these applications are often 100% flexible until the slurry is actually poured. In other words, traditional systems do not exactly provide the “right stuff” to handle the constantly changing needs of internal and external participants. And if internal systems challenges were
not enough, operating in an external environment also exposes participants to new collaborative business processes, diverse supplier application environments (AS 400s anyone?), and a greatly expanded set of security and liability concerns (not to mention the challenges of “shared” ownership of specific business processes). The good news, however, is that new approaches can leverage existing enterprise investments to create the necessary external interoperability at a fraction of the original cost. Figure 1, below, depicts some of the additional platform requirements that externally oriented environments require.

**Figure 1 External environments require additional types of platform capabilities**

In this new external environment, the core competency of A&D and manufacturing companies has changed from internally led design and manufacturing to knowledge coordination and business process management across an extended community of suppliers, partners and customers. And at the center of these new needs is information, visibility, and accountability. For example, consider how the definition of non-delivery risk has evolved, forcing manufacturers to accept new levels of responsibility, even when they have less control over operations and production than in the past. By sharing critical insight at all levels of the organization, however, companies can improve decision making while also mitigating risk. What makes this possible is gaining access to the right information, at the right place, at the right time across an extended supply network. This network centric approach to doing business is what enables organizations to gain situational awareness about all of the activity throughout their supply chain. Situational awareness can help executives and managers from different participating companies understand how their role and how decisions will impact their entire supply network. How do companies achieve situational awareness? To build this level of visibility and information sharing at all levels, it is necessary for A&D and manufacturing companies to undertake three key initiatives. These are:

1. Understanding and deploying a network approach to managing business processes and technology solutions
2. Embracing security and identity assurance programs which enable a secure foundation for visibility, collaboration, and management outside of the four walls
3. Building an action plan to roll-out and take advantage of new capabilities (while accounting for the internal and external change management required)

Throughout the rest of this paper, we will investigate how these three areas work together to drive success in an externally focused business environment and throughout extended supply networks. No one said opening the front door is easy. But with the right plan and approach, the transition can be much more seamless than it first appears.

**DEVELOPING A NETWORK CENTRIC APPROACH TO DOING BUSINESS**

When access to external information matters more than absolute process ownership, success comes from taking an approach that embraces shared standards and interoperability at all levels of the supply chain. This network centric approach enables both large and small organizations to gain competitive advantages based on their individual ability to leverage standardized processes and technology that works with all of their external partners—not by creating, owning and maintaining proprietary approaches that add cost and complexity to the community. A network-centric approach to doing business improves the functioning of the value chain through enhanced external collaboration, and
reduces cost by an efficient means of interoperability. For example, by requiring that individual organizations integrate with a single, common environment to reach a virtually limitless combination of partners and business networks reduces the costs and barriers typically associated with establishing and managing numerous different individual connections. They can help stakeholders sense and respond proactively to challenges within the supply chain before they have a negative impact. At the same time, a network centric approach can help organizations focus on exception management by automating the majority of external transactions and interactions, while also providing insight to help focus limited resources on the most strategic issues.

But an external business network is more than just an integration hub or an intelligent supply chain dashboard—it is a complex solution that encompasses enabling technology, security, content, and connectivity. Moreover, it enables visibility up and down the supply chain and across business processes and organizational boundaries. Figure 2, below, outlines a number of the most critical business needs in an external world, as well as some of the top challenges companies face in addressing these areas.

External applications can help organizations overcome an evolving set of risks within their supply chain. Take for example, the implications that real-time interoperability and visibility between organizations has for supply chain management. In a networked business environment, it is critical to have a foundation that provides a real-time information source for all participants. This "one version of the truth" in an external environment complements the internal systems of record that organizations deploy within their four walls. Building an environment that facilitates situational awareness for all participants also requires the ability for multiple parties to collaborate and work together in parallel, with an assurance that the platform will continuously update and process incoming information. In the networked world, the concept of serial information processing is anathema to building the speed and flexibility to compete effectively. To address the need for situational awareness from a value chain standpoint, there are three key business process areas that must be addressed. These are:

- Design and product collaboration (for coordinating and sharing product design, specifications, and other information with all partners within a supply chain)
- Procurement and strategic sourcing (for managing and optimizing costs with supply partners)
- Supply chain planning and execution (for gaining visibility and control to reduce risk in multi-tier environments)

It is critical to make the internal/external distinction in these three areas. The same set of capabilities that address internal enterprise processes are not as efficient when deployed in an external, multi-party environment. For example, a procurement application that provides search, requisitioning, invoicing, and payment capability should not require that an organization individually hard-wire every supplier into a one-off system. Rather, by leveraging a networked application, a procurement solution built for an external environment only makes suppliers connect a single time, greatly reducing costs for all participants. Also, by creating information exchange standards and workflows one can make managing the entire business process easily repeated and scalable across multiple buyer/supplier relationships. In contrast, traditional application environments that rely on core ERP/MRP capabilities—even in a web or client/server world—do not provide the same degree
of flexible integration or standard workflow to bring in external supply partners in a dynamic, networked environment.

There are a number of other advantages that a networked application can provide. The impact of a ready-set of enabled partners and supplier content allows participants to focus on developing advantages around important competencies (such as supplier performance management) rather than routine transactional functions. Just as a Bloomberg terminal in the financial services world enables traders and organizations to make more informed decisions and to model and execute their actions in a common system, networked applications in the design, procurement, and supply chain environments provide a similar advantage to participants by offering capabilities that enable connectivity, pre-configured processes, and critical information to all participants. Furthermore, a networked application provides security and autonomy to its users, lowering risk for all members and creating a neutral playing field for large and small members alike. And perhaps most important an external networked application can address the tail end of the supply chain, or the 80% of suppliers that make up 20% of the transactions. It is in this part of the supply chain where efficient process enablement matters most. Historically, adopting this “tail” has been very expensive, requiring buying organizations to “strong arm” participation of a vast number of their smaller suppliers, but also provide technical support and troubleshooting for their particular one-off solution.

THE STITCHING THAT HOLDS A NETWORKED APPROACH TOGETHER
By nature, a networked approach must rely on a “many-to-many” model that enables different organizations and individuals to play unique roles in specific programs and tasks. This approach provides unprecedented technology flexibility with low total cost of ownership for all participants relative to building and maintaining capabilities themselves. But it also brings new technical requirements, such as the need for an open, neutral, trusted infrastructure with applications to help companies reduce the time and costs required to incorporate new capabilities (and service level agreements that will have to exceed common internal IT commitments). For many new capabilities, the “build” or deploy internally option is simply not possible—even if cost is not a consideration. The time it would take to achieve material business benefits in an external environment are simply too long to warrant the “internal” option.

For many executives, these types of networks are more than just a new approach to managing existing business processes. Rather, they bring an entirely new mindset to overcoming challenges in an environment that is constantly evolving. The essence of a networked model is particularly strong because it unites information assets from all of its members in a common, extended architecture. To compete and grow in this world, it is first necessary to examine the external business process requirements required to work with key suppliers who have taken on new levels of responsibility. In many cases, this task requires changing the activities, management approach, and structure of the traditional organization (often in a dynamic, rapid manner). For example, the global thirst for specialized materials such as titanium and certain composite and aluminum components has led to rising prices and even shortages for key inputs in recent years. This has forced platform providers to take an active role in owning the procurement of key commodity inputs. This in turn requires new processes and applications that build demand and inventory visibility across an extended network, ensuring adequate supply for all participants.

Inefficiency and risk are also abundant in the case of global sourcing and operations initiatives where physical distances, time, and transportation barriers can introduce—and amplify—a range of challenges, both existing and new. For instance, the time from a supplier's distribution facility to the manufacturer's shop floor is often measured in weeks—and even months—in a global environment rather than days (or even hours) in a regional one. Of course expediting can solve this problem (assuming available capacity), but often at a significant premium. When supply performance challenges come up in this world, it is critical to have early visibility into potential issues before they can adversely impact the broader supply chain (and ultimately the end-customer). Without this visibility, companies introduce a new level of risk to their organization. And in complex, multi-tier environments, when a single supplier two or three
tiers down the chain has performance issues, an entire program can be delayed or jeopardized. The key to overcoming this risk involves building visibility and situational awareness that provide all supply chain participants with access to information throughout the design, purchasing, and manufacturing processes. In turn, this new level of insight could help companies make better decisions by providing new types of analysis into performance trends and issues, predictive insights into future problems, and proactive intelligence to make business decisions.

Figure 3 Mutli-tier business process and information sharing drives visibility and situational awareness.

Two of the most important defense platforms of the United States military in the coming decades will be the F/A-22 fighter (also known as the Raptor) and the Joint Strike Fighter (JSF). But the prime contractors in both cases are acting more in the role of program designer and manager than as lead manufacturer. For both planes, the majority of the fuselage, wings, stabilizers, avionics gear, cockpit systems, engines, engine controls, and landing gear are being built by third parties. In fact, nearly two-thirds of each aircraft is made by suppliers other than the primes.

Understanding and deploying the right set of business processes and technical solutions in an external environment is essential. But just as an athlete needs the right pair of shoes before running a marathon, it is just as critical to investigate and understand the “first principal” requirements of doing business in a networked world. Our experience suggests that deploying a secure, networked application environment that allows the exchange of product, operations, and transactional information in an external world is critical to success. In fact, AMR Research recently conducted a study that surveyed small and medium sized business which found that security remains a top hurdle for software as a service (the predominant architecture model for applications that exist between organizations). Hence, creating a secure environment with clearly defined rules, permissions, and authentication (built on top of processes and technology that validate user identities in a multi-company environment) is another essential step to enabling the external supply network.

UNDERSTANDING THE NEED FOR SECURITY AND IDENTITY ASSURANCE IN THE EXTERNAL WORLD
Manufacturers of all sizes have realized that supply chain risk—even if it is one or two steps removed from their direct operations—can wreak as much havoc as internal production risk. But effectively sharing the information outside of the four walls to better manage this risk can introduce significant...
security concerns. For all organizations, this is a new type of problem, and one in which traditional approaches (e.g., firewalls and internal security measures) are of little value. That is because regulations such as export control have everything to do with individual identity and location—even when global design and production collaboration is critical. In these environments, often the weakest link—and the biggest challenge—for security is identity management. “Do you know with absolute certainty who you are doing business with?” We can trace back nearly 90% of security problems to identity breaches because organizations too often focus on buying “security” solutions rather than making sure that security is built into each and every application they use. The cost for even inadvertent violations can be significant. For example, current ITAR (International Traffic in Arms Regulations) fines for individual security breaches where national security information is at stake averages over $16 million per occurrence in the US.

The fines associated with running afoul of regulations thanks to insufficient security and identity assurance is only a small aspect of the risk company’s face when doing business in a networked environment... For example, consider the case of a major tier one A&D supplier which was barred from supplying any material to government programs for 45 days because they purchased metals from a company on the denied parties list. The financial impact of the fine pales in comparison with the impact to this company’s reputation and brand equity. Ultimately, this violation not only hurt their bottom line, but impacted their customers who were now faced with program delays and material shortages...and potentially the end-users, our war-fighters on the front lines.

In both the global and domestic environment, security matters more than ever. Take, for example, the increasing trend in the defense industry towards global, “round-the-clock” design collaboration with teams in various countries. Ensuring that only the right level of confidential information is communicated to the right set of eyes in a global environment is critical to ensure that breaches do not occur. But even in non-defense areas, the preservation of intellectual property is a critical element of security and identity assurance programs.

Despite its reputation for rapidly developing a strong manufacturing base, China is also known as a poor defender of intellectual property rights. This puts the onus on those sourcing from the region to protect their intellectual property. Just as individual merchants and tradesman could not always count on “the law” to protect their property interests on the Western frontier in the eighteenth and nineteenth centuries, pioneering organizations sourcing from—and selling into—emerging markets must also take a similar, hands-on approach to securing their own interests.

Taking Preemptive Measures to Secure the Supply Chain

Even in other industries—which do not have to worry about ITAR (International Traffic in Arms Regulations) compliance—leaders are taking pre-emptive measures to secure their supply chains by tackling identity management based on geography. One global leader in the oil and gas world captures geographic information via GPS every time an employee logs onto their system from a remote location. This system relies on a global network infrastructure as well as embedded measures which are concealed in individual access devices.

Liability and business risk are also significant issues to consider when thinking about working in a networked environment. Here, it’s important to think about the questions which are raised from giving access to internal applications to users from other organizations. For example, do you know these individuals are who they say they are? Do you know enough about them to determine appropriate access to information? And how will you know when their status changes (e.g., when they move to a competitor, become unemployed or transition onto an unrelated project)? In the past, organizations have simply issued credentials to employees of their suppliers in order to share important information.
One major A&D company is estimated to have
issued 250,000 accounts to individuals from outside
their company for access to internal systems.
In addition to the huge liability concerns, this
company employs 35 people to manage these
accounts. As the need to collaborate with suppliers,
partners and customers grows, a networked
environment must address the issue of managing
individual identities in a way that provides the
required levels of trust efficiently and effectively.

When it comes to security, companies need
a framework that is consistent across various
businesses. By considering a single approach
and standard to security that satisfies commercial
and government requirements, A&D organizations
can streamline their processes and improve their
margins by making a single investment. While
new, this trend of embracing a common identity
management solution for commercial and defense
has a chance to grow as competitive and
cost pressures—not to mention shareholder
expectations—continue to rise.

To make this type of universal security a reality,
what is needed is a new type of networked
approach to security that provides a foundation
for trust. With this, information and transactions
will be able to securely flow between and among
partners. Bill Gates recently commented on the
power of these types of networks by noting,
“The trust ecosystem has to have a very rich
design, because after all, trust comes from many
sources... so it can't be something where there's
one unique piece of software, one unique
organization, but rather, it has to be totally
federated, so that all those trust statements
can be understood and reasoned against.”
The challenge of this approach is that it requires
a large scale effort to standardize not just
technology, but also information access profiles.
Perhaps the most simplistic analogy here is to
the global phone system, which provides universal
dial-tone and interoperability, despite varying
methods of network access and a huge diversity
of network infrastructure between nations.

In virtually all cases, it makes sense for organizations
to align with a trusted third party to build out this
type of networked security and identity assurance
to enable a secure foundation for commerce and
information exchange across organizations. Just as
organizations quickly realized that maintaining direct
point-to-point voice connections with all of their
partners, customers, and suppliers would prove
prohibitively costly (not to mention impractical),
companies are coming to the same when it comes
to external secure infrastructure today.

THE JOURNEY BEGINS:
PLANNING FOR A SUCCESSFUL MISSION

Even with a clear understanding of the business
process, technology, and secure infrastructure
requirements necessary to succeed in an external
environment, opening up the front door to the
outside world is never easy. The good news is that
companies do not have to set out on this journey
alone. As they take in the possibilities and risk that
the external world can bring, organizations can
improve their chances for success by identifying
the right set of partners who can guide their journey,
providing solutions, knowledge, and expertise to
ensure safe passage. The right partner can expose
a new world of opportunity to its customers, by
helping them mine, analyze, and examine the right
set of business information—both internal and
external—to make the most informed decisions at
all levels of the organization.

Companies can prepare for their external journey by
building a clear business case for investing in critical
enabling areas. By starting with a clear understanding
of external businesses processes—and the impact
that a new group of participants will have on specific
functions—A&D manufacturers can ground their
application and platform decisions based on specific
needs, rather than the sales pitch of an individual
provider. At the same time, it is important to develop
an understanding of other organizations that have
gone down a similar path before—sometimes in the
same industry, but often in others. These types of
examples can help illuminate the best route on a
specific journey, pointing out dangers and pitfalls
before it is too late.
It is critical to have a plan that achieves short-term objectives while also keeping a longer-term goal and signpost in sight. Ensuring that there is some type of payback—or measurable benefit—in a period of months, rather than years, is an important enabling factor in the success equation. The good news is that there are a range of additional benefits—in addition to procurement and supply chain success—that come from enabling such capability as multi-tier visibility and management. These additional benefits include enhanced security, a new level of data portability across applications, and the ability to improve data-intensive business decisions that cross functions inside an organization.

**TAKING OUT THE COMPASS AND CHARTING THE COURSE**

Partners and advisors are often invaluable in helping organizations understand where to get started—and how to prioritize specific investments along the way. But a quick exercise can help A&D organizations develop a basic understanding of their current and emerging needs based on their specific business environments. Figure 4, below, can help your organization understand where it sits on the external supply network adoption curve.

For the above diagnostic, organizations that answer “yes” to more than half of these questions are furthest along on the adoption curve and require the most advanced technology, security, and infrastructure to support their current and emerging external business process needs. Companies that answer “yes” to fewer questions are lower on the curve, but should still prepare for the impact that the external supply network will have on their business, planning for investments based on targeted needs.

Understanding the “you are here dot” is a critical piece to getting started on the external supply network journey. At the same time, appreciating what future developments will bring is just as important. The external supply network of tomorrow will continue to provide a core set of security and applications to facilitate a full range of internal and external business processes. It will also move beyond helping just coordinate product designs and production scheduling. It will even transcend multi-tier collaborative sourcing and visibility. The external supply network of tomorrow will help create a new

---

**Figure 4 How Dependent is Your Organization on the External Supply Network Today?**

If you answer “yes” to more than half of the questions, we would recommend consulting an outside partner to understand your current and emerging supply network needs.

1. Are we struggling in anyway to adopt our revenue models to the changing economic needs of the marketplace (e.g., power by the hour, end of cost plus, etc.)
2. Are our customers demanding increased flexibility (e.g., pricing, terms, lead-times, configurations, etc.) despite rising platform complexity? Are we now responsible for work previously done by our customers?
3. Are we sourcing from, selling into, and servicing our platforms in global markets? Are we managing inventory and / or working with another party (e.g., a 3PL) for global delivery?
4. Do our suppliers play a key role in platform design?
5. Do we manufacture less than 50% of the parts and assemblies that go into our platforms?
6. Are we still looking for a C-Level Executive to champion the business value that external supply relationships can bring?
7. Would we classify our need to secure information both from an IP and regulatory perspective as high?
8. Do we need to put programs in place to understand the total cost of ownership of each component we make or source in our extended supply network? Do we need visibility into multiple-supply tiers?
9. Could we make use of an early warning system to reduce supply risk and identify supplier issues (e.g., low inventory at a key point in the supply chain) before it becomes an issue?
10. Have we reached the limits that our internal systems (e.g., ERP, MRP) can support in facilitating external collaboration across business processes (e.g., design, sourcing, operations, service parts management)?
type of A&D provider, bridging the full set of integrated processes that start with a mouse-click on an engineer's desktop and end with the supplier's bank account. It will provide both business process efficiency and information efficiency to large and small network participants. The result will be a massive increase in flexibility and information transparency throughout the extended supply chain, and a new level of situational awareness for all participants.

**GLOSSARY**

**External Interoperability**  
External interoperability is the result of business systems and processes that integrate and work together outside of the four walls of the organization, crossing organizational boundaries and functional areas.

**Identity Assurance**  
Let's leave this one for Jeff

---

**What’s Possible? 2008: The “Virtual” OEM**

Imagine that it is 2008 and a large global systems integrator has moved even further away from its traditional manufacturing role. From product design through to service parts management, the OEM has shifted responsibility for the majority of its functions to partners. It now considers its primary competencies as marketing, financing, partner coordination, and customer service. As an example of how far the company has come from its roots, for a higher volume platform in its commercial business, the company has even moved away from in-house final assembly, preferring to outsource this function to new JV partners in Central Europe and Asia.

To help bring platforms to market more quickly, the OEM has invested heavily in systems and processes to facilitate collaborative engineering and production across hundreds of supply partners. This has become even more critical, as its customers are demanding a new level of flexibility to change their orders (which must cascade down to all participants within the supply chain). The company’s entire design, procurement, and planning capabilities are built on a Federated identity management system to ensure trust and security in a virtual environment. In what has become a commonly quoted line, Aviation Week editorialized that despite the “open-door data sharing and collaboration environment, that the OEM’s data and competitive secrets are more secure now than ever before.”

Despite an increasing reliance on partners in taking a lead role in all stages of production, the OEM has taken on new—and some say more active—roles in sourcing and supply chain management. To ensure continuity of supply and optimal pricing, the company has increasingly bought raw material inputs such as titanium and composites resin on behalf of its supply community. And thanks to the OEM’s technology and process investments, all supply partners have around the clock visibility into relevant information such as inventory levels and machine capacity to reduce the risk of supply disruptions. Many access this information via embedded devices such as cell phones and pagers, and are proactively alerted to potential issues before they arise. Third party logistics providers (3 PL’s) are also playing a new role as well, helping not only to reduce the cost of global transportation, but managing inventory and ensuring continuity of supply.

This is one example that shows how an OEM will increasingly rely on its external supply network in countless new ways in the coming decade. By shifting its core competencies away from internal management to external enablement, the OEM will thrive despite the complexity and interdependencies of moving outside of its four walls.
Imagine that it is 2010, and the defense needs of the world's superpowers have evolved once again. With never-ending instability in the Middle East and the continued boom of China, India, and Pakistan—not to mention a new set of crises in North Korea—US and European military resources have become stretched on numerous fronts. These demands have worked their way into the defense industry, which is increasingly being tasked with coming up with creative solutions and platforms in a fraction of the time of past programs.

One defense insider was heard remarking that he trusts his contractors more for their ability to manage a group of worldwide suppliers to deliver programs on-time and on-budget than for their systems design or manufacturing prowess. In this environment, defense leaders have realized that their ability to serve as a general contractor whose primary role is to coordinate supply partner activity is a prerequisite to winning highly sought after contracts. This has resulted in a new round of technology investments designed to drive collaboration and coordination among partners. The highly sensitive nature of specific programs and the critical role that online communication, information sharing, infrastructure, and application security play has made technology a dominant topic of conversation in the halls of both the IT organization and the executive suite.

Given the huge task of securing information across tens of thousands of external individuals and hundreds of companies, many contractors have turned to neutral authorities to manage an underlying secure infrastructure. Supply networks provide a foundation of information security and identity management to ensure that only project participants with the right set of current credentials can access information to their individual role in the specific programs.

In this scenario, identity-based platforms and collaborative infrastructure enable defense contractors to differentiate themselves based upon the capabilities and business processes they manage on top of an industry standard security layer. The common network model provides connectivity and a "security dial tone" that can make the accelerated program development needs of the US and other governments a reality.
**Power-by-the-Hour (PBTH)** Under PBTH programs, A&D customers (airlines or governments) pay a fixed amount per flight hour in exchange for the delivery of a service or solution (e.g., platform, maintenance, repairs, etc.) under a pre-defined set of programs. These contracts help customers “fix the cost” of service based on estimated usage.

**Supply Network** Supply networks enable buyers and suppliers to connect a single time to a common environment to transact and share information. They reduce the cost of doing business by alleviating the need for establishing and maintaining expensive, proprietary point-to-point connections.