Preparation for the launch of PeopleSoft v9.0

An overview of the coming changes and how they affect you

On Monday, June 21, Sandia will launch the much-anticipated upgrade to its human resources information system, known as PeopleSoft. This upgrade is designed to introduce a modernized, simplified PeopleSoft system that serves the Labs’ Human Resources functions in the most efficient, simple, and cost-effective ways possible. In the new system, PeopleSoft users will see changes in both appearance and functionality and help is available to guide users through this transition.

In conjunction with the information that has (Continued on page 6)

Cyber bad guys get smarter, Sandia defenses get stronger

How to counter both known and unknown threats

The Lab News recently interviewed three members of Information Technology management: Chief Information Officer Art Hale (9640), Acting Director of Computing & Network Services 9300 Tom Kickner (who is also senior manager of Computer Support Unit Services 9340), and Carol Jones, senior manager of Cyber Security Services & Technologies 9310.

Lab News: We frequently hear that the cyber threat is significantly more serious than a decade ago. What’s worse about it now? Why is this a more dangerous environment?

Art Hale: A lot of people have learned a lot of things over the past decade. Software designers have learned how to create better software, and the people who want to exploit our current operating environment have also learned a lot about its weaknesses, its vulnerabilities, how to attack it and compromise it.

L.N.: Are you talking about people we usually call hackers? High school or college students doing it for fun?

Art: I’m talking partly about them, but a more serious threat to Sandia’s work environment is nation-state adversaries that target a place like Sandia because of the kind of work we do, nuclear weapons and other national security applications. They’re interested in our most sensitive information. They use all the mechanisms at their disposal to try to find out as much as they can. So we’re facing very sophisticated attacks.

The second thing that has happened in the past decade is that much of what we do has moved to the Internet. People need to interact across the Internet, they need to find and access information over the Internet. They find it from all kinds of places using search engines, and the adversaries who want to attack us know that and exploit it. They can compromise machines elsewhere that have information that we might be interested in — we may just happen to be there, or there may be something that’s close to us. An employee of Sandia might access the website of a local TV station, or something at a university near by, for example.

State of the Labs 2010

PASSING THE TORCH — Labs Director Tom Hunter, left, and Paul Hommert, who will become Sandia president and Labs director on July 9, answer questions from the media ahead of the 2010 State of the Labs presentation at the National Hispanic Cultural Center Tuesday evening. Tom talked about the challenges of maintaining the nuclear weapons stockpile, cyber security, terrorism, energy, and economic competitiveness. He then turned the presentation over to Paul, who discussed an “exciting” future for Sandia as its mission diversifies and paid tribute to Tom. More in the next Lab News. (Photo by Lloyd Wilson)

Admiral’s talk explores security implications of climate change

The US Navy views climate change as a challenge, intends to prepare for it, and would appreciate help from the national labs, Rear Adm. David Titley told an attentive CNSAC audience in an unclassified lecture titled “Climate Change and National Security”. The lecture, simulcast to Sandia/California, is the first of a group of lectures intended to explore the national security implications of climate change, says Bob Leland, director of Computation, Computers and Math (1400), whose center arranged the talk under the leadership of John Mitchiner (1430) through Dw 8000 VP Rick Stulen’s Energy, Climate and Infrastructure Security SME.

Titley, the Navy’s oceanographer and navigator, is senior policy adviser to the chief of naval operations for issues relating to national ocean policy and governance, as well as (Continued on page 4)

Inside

Sandia team scrambles, gets creative, to help NASA ensure safety of recent space shuttle Discovery flight. Read all about it in a first-person account by LOIS project lead Jose Rodriguez …………………. 7

Also …

Classes offered to help Sandians become entrepreneurs ………… 2

A new approach to energy security ……………………………… 4

Simulating a “virtual” nuclear reactor …………………………… 8

See also . . .

Peeling the onion of malware: A Laboratory Directed Research and Development (LDRD) project to understand and develop countermeasures for malware and botnets. Page 3

Bright future for cloud computing: What is cloud computing, and what might it mean for Sandia? Page 5

The coming change in health care benefits: How will it affect you and your family?

Sandia Total Health out-of-pocket maximum. See page 9.
That's that

I'm a bit of a word buff—Who knows, right?—and always get a kick out of watching the language evolve. I find English remarkable in its adaptability and flexibility. It seems to me that there's a deeply pragmatic strain hardwired into the language. I think that's why people who work in it make it, use it, and make it your own regardless of its national origin. Not being bilingual is a negative. It's more like a minus. It's difficult to work in languages when you speak them as easy in their virtue as is English. Maybe lots of them are. Spanish speakers incorporate English words into their conversation all the time, for example.

This is why we have the equivalent of the Académie Française, which for three centuries has been fighting the good fight to keep French free of foreign words. And especially English words. Incredules is the word. Results of its deliberations are published as official law, laxely enforced, to be sure, but still. (All we have is those seven words you can't say on TV.)

Here's one of the things I like about my native tongue: We just borrow words from other languages...we make them up with dizzying abandon. I actually find myself reading it for pleasure sometimes. (I know, I know.)

The other day, I got an email from AF. Periodically they send out notes updating use and style questions. This note is a list of words related to social media. (AF by necessity has to keep up with the language as it is actually used. Often, of course.) Among the words: retweet, unfriend, crowdsourcing, wiki. Even familiar words have new meanings and usages: fan, follow, avatar, handle.

I've got all these words to talk about things that didn't even exist a decade ago and now they're totally assimilated into our society.

There's a lesson here: when something is useful—the web, or social media, for example—it will quickly integrate it and create an English language around it. And it will be very, very difficult to make them stop. Once Facebook enters the language it isn't going anywhere. The converse is probably true, too: if something isn't useful, it's probably going to be very hard to make people adopt it.

That's why the French language police are always fighting a rearguard action: French speakers and certain English words are encroaching on the language...and those then, language purists notwithstanding, I do sympathize with the effort, though. Perhaps it's time for a "rapprochement" with our French-speaking cousins: we won't use any of their words if they don't use any of ours. (Definitely more English words, definitely less French.)

...One of the hardest things we do—and I think one of the most important—is to publish obituaries about on-roll employees who pass away. I call them "obituary," but they're probably better described as memorials. We don't try to provide a comprehensive summary of an individual's lifetime. We say, if a forum where colleagues and friends can offer a few reminiscences. We’ve been told the memorials mean a great deal to our families...what we lose is a member of the family. And perhaps it’s not surprising that surviving family members often consider us— fellow Sandians—as members of a big, extended family. Case in point: Rose Salas, sister of Fred Salas, the employee who we lost a while ago. She and her family, and those then, language purists notwithstanding, I do sympathize with the effort, though. Perhaps it's time for a "rapprochement" with our French-speaking cousins: we won’t use any of their words if they don’t use any of ours. (Definitely more English words, definitely less French.)

One of the hardest things we do—and I think one of the most important—is to publish obituaries about on-roll employees who pass away. I call them “obituary,” but they’re probably better described as memorials. We don’t try to provide a comprehensive summary of an individual’s lifetime. We say, if a forum where colleagues and friends can offer a few reminiscences. We’ve been told the memorials mean a great deal to our families...what we lose is a member of the family. And perhaps it’s not surprising that surviving family members often consider us—fellow Sandians—as members of a big, extended family. Case in point: Rose Salas, sister of Fred Salas, the employee who we lost a while ago. She and her family, and those then, language purists notwithstanding, I do sympathize with the effort, though. Perhaps it’s time for a “rapprochement” with our French-speaking cousins: we won’t use any of their words if they don’t use any of ours. (Definitely more English words, definitely less French.)

...One of the hardest things we do—and I think one of the most important—is to publish obituaries about on-roll employees who pass away. I call them “obituary,” but they’re probably better described as memorials. We don’t try to provide a comprehensive summary of an individual’s lifetime. We say, if a forum where colleagues and friends can offer a few reminiscences. We’ve been told the memorials mean a great deal to our families...what we lose is a member of the family. And perhaps it’s not surprising that surviving family members often consider us—fellow Sandians—as members of a big, extended family. Case in point: Rose Salas, sister of Fred Salas, the employee who we lost a while ago. She and her family, and those then, language purists notwithstanding, I do sympathize with the effort, though. Perhaps it’s time for a “rapprochement” with our French-speaking cousins: we won’t use any of their words if they don’t use any of ours. (Definitely more English words, definitely less French.)

One of the hardest things we do—and I think one of the most important—is to publish obituaries about on-roll employees who pass away. I call them “obituary,” but they’re probably better described as memorials. We don’t try to provide a comprehensive summary of an individual’s lifetime. We say, if a forum where colleagues and friends can offer a few reminiscences. We’ve been told the memorials mean a great deal to our families...what we lose is a member of the family. And perhaps it’s not surprising that surviving family members often consider us—fellow Sandians—as members of a big, extended family. Case in point: Rose Salas, sister of Fred Salas, the employee who we lost a while ago. She and her family, and those then, language purists notwithstanding, I do sympathize with the effort, though. Perhaps it’s time for a “rapprochement” with our French-speaking cousins: we won’t use any of their words if they don’t use any of ours. (Definitely more English words, definitely less French.)
Malware 101... and botnets, too

Malware is short for malicious software, a term that encompasses what is commonly known as computer viruses, worms, Trojan Horses, and spyware. Over the past 20 years, computer viruses have gone from being annoying—in some instances, more akin to graffiti tagging—to downright lethal. Not coincidentally, that’s the same time frame in which the Internet went from being limited to universities to being ubiquitous. According to the website Internet World Stats, in 2000, 3.6 million people used the Internet, as of September, that number had jumped to 1.7 billion.

Malware is ubiquitous and moves at lightning speed; it is common for a newly installed computer running Windows XP to be infected within 10 minutes of being connected to the Internet.

Once installed, no longer resisting the inner Malware is used to collect information about the user’s behavior, which can be used to display intrusive pop-up ads or record keystrokes to steal usernames and the other sensitive information. Or, malware can be used to turn a computer into a zombie computer (a more technical term is “compromised computer”) and used as part of a larger network of like computers (hence the term botnet, for robot network) to wreak havoc on the Internet.

In the early days, botnets seemed to be writing malware more for bragging rights about how many computers their virus could spread to and how quickly. Today, there are financial reasons to spread malware and build the largest possible botnet, Ken explains. “There is an underground economy built around botnet ‘owners’ renting their botnet to the highest bidder, who might use it to blackmail a company by threatening to take down their website.”

The organized crime element of the botnet world has led to a curious Wild West environment on compromised computers. Recently, Ken’s father suspected his computer might have been compromised and asked him for help. Ken found that the computer was indeed compromised many times over.

“His computer was essentially a zombie computer with 80 different viruses fighting it out for control,” Ken says. “Malware is now being written to not only take control of a computer, but defeat any other malware that is already there doing the same thing.”

Despite the “Whaa-a-Mole!” nature of combating malware, Ken thinks the efforts of many others in the field, are making serious inroads. And, he finds the work very gratifying.

The work builds on research led by Ron Minnich (8961). Last year, he demonstrated the ability to run more than a million Linux kernels on virtual machines (Lab News, July 31, 2009). The researchers plan to take two approaches: emulating the properties of a Windows system sufficiently to modify a large number of random malware to observe and reducing the size of Windows. “The size of Windows is a significant hurdle in getting to a million nodes,” says Jamie. “Right now for every 10 instances of Windows, you could probably boot a thousand instances of Linux.”

Sung Tzu said it first, in the sixth century: “Know thy enemy.” In The Art of War, Tzu write that to be a great general, “You must come to understand his methods from the vantage point of command control could look at the other end of the spectrum. “We’re proposing a new LDRD to boost a million monitored nodes and study large-scale behavior of bots,” Jamie says. “Things happen at that scale that you just can’t see even with 10,000 instances.”

The researchers learned that quickly disabling protective mechanisms is a key step to understanding and developing countermeasures for malware and botnets (see “Malware 101 and botnets, too”). To reverse engineer the malware, Ken used three different technical approaches: static analysis, dynamic analysis, and emulation. Malware authors wrap their code in defensive layers to obscure their true purpose and prevent reverse engineering. For example, a code may not run linearly, meaning it jumps around seemingly randomly among a million lines. Or, designers modify a program so that parts of the code modify other parts so that its real purpose is not readily apparent. Some malware is designed to detect when it is being run and watched, and alter its behavior. The researchers learned that quickly disabling protective mechanisms is a key step to understanding and stopping the spread of malware. Ken can now unwrap a piece of malware in about a week, a process that took several months at the start of the LDRD. He’s beginning a late start LDRD that aims to use FARM to automate that unwrapping process — an “everything-but-the-kitchen-sink” tool that would be integrated into FARM.

After three years studying botnets on a small scale—from one to 40 hosts—at Sandia and at a number of other government agencies.

“As more people use FARM, we can take what they learn and continue to improve the entire package,” Jamie says.

The team chose to investigate Storm and Waledac, two complex, pervasive, and long-lasting botnets. Storm is said to be responsible for up to 20 percent of the world’s spam at its heyday, infecting up to a million computers by some estimates. Waledac, considered by many to be a second iteration of Storm, infected hundreds of thousands of PCs worldwide and was thought to be capable of sending more than 1.5 billion spam messages a day. Through its Digital Crimes Unit, Microsoft Corporation effectively shut down Waledac last year, a major victory over the malware underworld.

To get to the core of the malicious software, Ken painstakingly worked to defeat multiple protection mechanisms. “The amount of work is asymmetrical,” he explains. “It’s easy to put on the protection mechanisms, but it takes a tremendous effort to take it apart.”

To reverse engineer the malware, Ken used three different technical approaches: static analysis, dynamic analysis, and emulation. Malware authors wrap their code in defensive layers to obscure their true purpose and prevent reverse engineering. For example, a code may not run linearly, meaning it jumps around seemingly randomly among a million lines. Or, designers modify a program so that parts of the code modify other parts so that its real purpose is not readily apparent. Some malware is designed to detect when it is being run and watched, and alter its behavior. The researchers learned that quickly disabling protective mechanisms is a key step to understanding and stopping the spread of malware. Ken can now unwrap a piece of malware in about a week, a process that took several months at the start of the LDRD. He’s beginning a late start LDRD that aims to use FARM to automate that unwrapping process — an “everything-but-the-kitchen-sink” tool that would be integrated into FARM.

After three years studying botnets on a small scale—from one to 40 hosts—the researchers now want to

The Forensic Analysis Repository for Malware (FARM), created by Jamie Van Randwyk, Ken Chiang, and Levi Lloyd, enables computer security personnel to triage malicious software within minutes, giving them an advantage in the fight against cyber attacks. Here Levi examines FARM’s analysis of a variant of the Waledac botnet. (Photo by Randy Wong)

Automating the process of stripping protection mechanisms might be one way to do this. “With FARM, that process is fully automated and takes only a few minutes of being connected to the Internet. Once installed, a Malware is short for malicious software, a term that encompasses what is commonly known as computer viruses, worms, Trojan Horses, and spyware. Over the past 20 years, computer viruses have gone from being annoying—in some instances, more akin to graffiti tagging—to downright lethal.

Not coincidentally, that’s the same time frame in which the Internet went from being limited to universities to being ubiquitous. According to the website Internet World Stats, in 2000, 3.6 million people used the Internet, as of September, that number had jumped to 1.7 billion.

Malware is ubiquitous and moves at lightning speed; it is common for a newly installed computer running Windows XP to be infected within 10 minutes of being connected to the Internet. Once installed no longer resisting the inner

Malware is short for malicious software, a term that encompasses what is commonly known as computer viruses, worms, Trojan Horses, and spyware. Over the past 20 years, computer viruses have gone from being annoying—in some instances, more akin to graffiti tagging—to downright lethal.

Not coincidentally, that’s the same time frame in which the Internet went from being limited to universities to being ubiquitous. According to the website Internet World Stats, in 2000, 3.6 million people used the Internet, as of September, that number had jumped to 1.7 billion.

Malware is ubiquitous and moves at lightning speed; it is common for a newly installed computer running Windows XP to be infected within 10 minutes of being connected to the Internet. Once installed no longer resisting the inner
US Navy

(Continued from page 1)

as navigation policy and standards. Mixing humor and environmental charts from the Applied Physics Lab at the University of Washington, Titley said the Navy was concerned that ocean levels would rise “a meter or two” over the next century, the result of the accelerating melting of the Greenland ice sheet and continued melting and thinning of Arctic ice.

“Why does the Navy care about this?” he asked. “We tend to build our logistic out here. It’s a Navy thing,” he said straightforwardly.

Faced with a situation that might require building dykes around its bases, the Navy reacts, he said. Navy oceanography cannot be “just scientifically cool,” it must have a practical outcome that transforms information into decisions. Otherwise, Titley said, imitating an impatient interrogator, “Tell me again why you’re here?”

By Shannon Guess (12150)

“Creating Focus in Turbulent Times.” That is the theme of Sandia’s FY 2010 Strategic Plan, a theme exemplified by the challenges the nation faces in a wide range of energy-related issues.

Consider: The US today is confronted with an unprecedented environmental crisis in the Gulf of Mexico, relentless cyber attacks threatening the electrical grid, foreign oil expenditures weakening the national economy while directly funding US adversaries, and the potential specter of climate change threatening the world we know.

What can Sandia do to help? How can the Labs focus its resources, expertise, and partnerships to best contribute? Sandia’s newly created Energy Security Thrust was established specifically to address these questions.

Transcending traditional programmatic boundaries

The objective of this thrust, along with the cyber and nuclear thrusts, says Terry Michalko (6300), leader of the Energy Security Thrust, is to transcend traditional programmatic boundaries, by drawing on expertise and capabilities housed across the Labs to best produce solutions to significant, complex, systems-level problems.

“We must take a more systematic approach to focusing our internal capabilities in energy security, systems engineering, and security approaches on key energy security challenges,” says Terry.

Just as Sandia has provided systems-level solutions for the nuclear weapons enterprise, he says, the Energy Security Thrust will use core capabilities to develop and strengthen the Labs’ role in informing the nation’s energy security strategy. Drawing on the Labs’ achievements in energy-based work, the Energy Security Thrust is uniquely equipped, Terry says, to address systems-level energy security challenges on three main fronts: reducing oil dependence, assuring operational energy, and strengthening our energy security and reliability.

“Each day, the US spends almost $1 billion importing oil from other countries,” says Andy McInroy, senior manager in Chemical Sciences Dept. 8530 at Sandia’s Combustion Science Lab. “Our country’s vast dependence on fossil fuel makes our economy and national stability increasingly vulnerable.”

High prices for fuel, competition for limited resources, increased risk of global climate change, and threats to political stability are some of the dangers posed by a dependence on fossil fuels. To address these challenges, the Energy Security Thrust is developing solutions such as advanced research in combustion efficiency, alternative fuels, and developing safer, more reliable batteries.

The second focus of the Energy Security Thrust is ensuring operational energy. A reliable energy infrastructure is the foundation of any essential operating system. Systems such as military facilities require reliable energy infrastructures to ensure mission readiness. However, energy infrastructure is vulnerable to both physical and cyber threats.

Providing microgrid technology to military bases

“The past is marked by a lack of coherent energy security and reliability strategy with regard to secure microgrid development in military installations,” says Dan Ronneau (5340), program director for Sandia’s Homeland Defense/Force Protection.

“However, Sandia is actively engaged in providing microgrid technology to military bases, as well as developing and testing other technologies to better integrate alternative energy into mission-critical operating systems.”

In the area of ensuring operational energy, Sandia is developing new technologies to improve component and system reliability, advance cost-effective energy storage, and improve cyber secure smart controls.

Climate change assessment is the third focus area of the Energy Security Thrust. As the challenges of energy security continue to rank as high priorities in national security strategy, Sandia’s new Energy Security Thrust will work with the NNSA Sandia Site Office and the KAFB installation commander to address issues of global vulnerability mitigation as well as adaption.

“A new approach to energy security mission

As the challenges of energy security continue to rank at high priorities in national security strategy, Sandia is more important than ever, says, for Sandia to initiate a new approach to fulfilling its energy security mission.

Specifically, the Energy Security Thrust will work in enabling systems science, identifying and mapping customers’ energy networks to assess future vulnerability to climate change, and identifying potential policy and regulatory changes. The thrust will also work on specific policy issues that Sandia can inform, and implementing a communication strategy engaging both internal and external stakeholders. Combining capabilities, resources, and talent from across the Labs, the Thrust can address energy security challenges more effectively, providing better solutions to our customers, Terry says.

“Connecting Sandia’s programs to the Energy Security Strategic Thrust gives us a broad positioning to better serve our customers,” says Dr. 8000 VP Rick Stulen, champion of the Energy Security Thrust. “We will be able to devise appropriate and effective research solutions to meet the complex set of energy and climate challenges they face in the coming years.”

Energy security at Kirtland AFB

In April, Sandia launched a study to evaluate Kirkland Air Force Base’s (KAFB) electric power system. The goal is to develop approaches to improve the base’s energy security and reliability using the Sandian-developed Energy Scurity MicrogridTM (ESM). ESM is a risk-based methodology enabling the base to use renewable energy resources for environmental benefits while also increasing energy security and reliability and enhancing critical mission assurance.

“The results of this study will allow us to better understand the actual impact of power interruptions to Team Kirkland and how we can ensure energy security for our most critical missions,” says Col. Robert Maness, 37th Air Base Wing commander.

Following the assessment, scheduled to be completed by October, Sandia will work with the NNSA Sandia Site Office and the KAFB installation commander to assess technology investments needed to improve the base’s operational readiness, enhance mission assurance, and extend the duration of energy system performance.

REAR ADM. DAVID TITLEY, Oceanographer of the Navy, is seen here on the right in a recent Navy ceremony in Washington. Titley spoke at Sandia about climate change and its potential impact on the Navy. (US Navy photo by John F. Williams)

He said the problems the Navy anticipates over the next century, after engaging nearly 400 people from more than 130 organizations to help gather data, include:

- environmentally forced or opportunistic changes in shipping routes,
- political problems as islands disappear beneath rising seas or ports become lower than sea level,
- increased economic activity in areas currently off-limits because ice at present blocks maritime access, and
- possible negative effects on plankton when the salinity of the ocean changes.

“Where will one billion people who get their protein from the ocean get it when the tiny living things that form the base of their food chain disappear?” he asked.

There was also, he said, “the human dimension that I’m not sure the policy folk always think about: humans want to stay where they are,” regardless of the alteration of the environment about them.

He predicted partnership opportunities and new energy security initiatives.

So, he said, he was interested in partnering with the national labs to develop better operational decision-making capabilities with respect to climate change.
Cybersecurity

Having gained a foothold on those machines, the adversaries can plant programs that compromise the machine. So when we go there with a simple query, a security team works diligently to introduce new processes files retrieved through the Internet.

We also monitor our network to look for patterns of behavior. We know how to detect with malicious code. We see two or three a month on average that a computer becomes compromised. And of course we then clean it up.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we're now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That's on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there's always something about which we don't know.

LN: What do we do about what we don't know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we're doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps. making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It's not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Bright future for cloud computing

During a discussion of cyber threats and upcoming software changes, Art Hale (9600) and Tom Klitsner (9500) also looked into how closer future might make a cloud service more distant future may not terribly distant. What is cloud computing, and what might it mean for Sandia?

Tom says, “There’s a natural evolution that information technology providers and their users will take. The web has changed the way we do everything in information technology, and will continue to do so. Companies like Google have made the case that the computing model of the future could put your computing capabilities on the web rather than within your own local desktop. Wherever you access it, it becomes Sandia’s local web. We wouldn’t be able to operate without the applications that run from there — timeliness, expense reports, and so on. There’s also a lot of advantage to running Office-type applications on the network. Your data and your software would reside on the network and would be accessible anywhere you go. If you need to share that information with others, it’s more accessible than if it were stored in your own computer. And even your data is owned. We have a sequence of changes that will happen as we move to the data center, and as the needs of the business, the mission, also evolve. We’re going to enable a lot of applications and services. We’ve studied the co-location of databases. We can make that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.

Art: We see things coming in that compromise a computer, probably a dozen times a week. We catch a lot of things that could have compromised a machine, because we’re now exploiting the application.

And then of course there are all the attacks hitting the perimeter. That’s on the order of hundreds of thousands a day. Perimeter defenses keep out the sophisticated attacks.

These are the kind of things that we know about the attacks. Of course, there’s always something about which we don’t know.

LN: What do we do about what we don’t know? Art: One thing is to deploy a more secure operating system for the majority of our work force, and we’re doing that. Windows 7 is much more secure, particularly the 64-bit version. It has a lot of features that use the power of the hardware to check software coming in. So if we have hardware that is a lot more secure, we can exploit that operating system.

So introducing Windows 7 and Internet Explorer 8 is one of the first steps.

making that the default operating system for new machines that come into the Labs and any rebuilt machines. We would like to move aggressively from Windows XP to Windows 7. It’s not just about the technology, but it is also about the capabilities because we have so many thousands of computers that are running Windows XP today. At some point in the future, at a date we have not determined, we expect to sunset all legacy operating systems, including XP, or quarantine those that need to continue to exist.
PeopleSoft (Continued from page 1)

**Time charging increments in PS v9.0**

<table>
<thead>
<tr>
<th>TRC</th>
<th>Exempt Employees</th>
<th>Time Incr.</th>
<th>Non-Exempt Employees</th>
<th>Time Incr.</th>
<th>Represented Employees</th>
<th>Time Incr.</th>
<th>Refer to contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>241 – Vacation</td>
<td>1 hour</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>Refer to contract</td>
<td></td>
</tr>
<tr>
<td>252 – Sick</td>
<td>1 hour</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>Refer to contract</td>
<td></td>
</tr>
<tr>
<td>263 – Share</td>
<td>1 hour</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Refer to contract</td>
<td></td>
</tr>
<tr>
<td>290 (as well as 291, 292, 294, 295, 299) – Corporate-wide Mandatory Training</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>Refer to contract</td>
<td></td>
</tr>
<tr>
<td>FTC</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Refer to contract</td>
<td></td>
</tr>
</tbody>
</table>

*All other TRCs refer to the applicable Corporate Policy.*

The T&L application will use time reporting codes instead of A-Orders. This is just a change in terminology; T&Ls will serve the same function as A-Orders have previously.

### Corrections

After the implementation of PeopleSoft v9.0, employees will not be able to electronically correct timecards that were previously submitted in ETR. The process will be similar to the current process used in the vacation and flex timecard applications. Corrections will be processed through the T&L application. If there is an incorrect timecard on a timesheet submitted in ETR prior to Monday, June 21, Payroll will only accept paper timesheets for corrections of the weeks ending May 27, June 3, June 10, and June 17.

### Time allocation

Time allocation previously existed as an optional time-tracking process available to department managers, team supervisors, and authorized office assistants and staff members. This feature enabled these individuals to have the timecard application functionally divide up or allocate projects and tasks based on the time charged for a work week. Time allocation will be discontinued with the implementation of PeopleSoft v9.0. Every employee is expected to charge his or her time to the appropriate project and task. Everyone should charge work directly to the benefitting project.

For additional guidance regarding time allocation, see the Payroll homepage.

### Extended work week

The extended work week (EWW) — when straight time hourly pay is more than 40 hours in a week for exempt employees — will require a vice president’s approval, which is to be obtained by an employee’s manager. Time charged to the EWW time code then requires weekly approval by the employee’s manager, and will not be compensated unless this approval is received.

### Action item

**Payroll**

**Beginning the timecard for the week of Friday, June 18, through Thursday, June 24, employees who are currently approved for EWW will begin charging time in excess of 40 hours to the EWW time code. Managers must approve any time charged to the EWW time code by 7 p.m. on Thursday of each week for the employee to receive EWW pay.**

**Vacation**

New-hire employees will receive a vacation balance immediately if they are on-rolls as of a pay period end date. Additionally, accrued vacation will now be credited to employees’ vacation balances twice monthly, instead of once monthly.

The PeopleSoft upgrade has been delayed until further notice due to issues with the PeopleSoft implementation. The upgrade will be completed in stages to minimize impact on users. The PeopleSoft upgrade is expected to be completed by the end of June.

**Eligibility**

Employees who participate in the Vacation Buy program will no longer have to exhaust all available balances in their Vacation and Flex accruals before using their bought vacation.

**Transition assistance**

If you have any questions regarding the upgrade prior to the launch, contact the project team at wg.upgrade@sandia.gov. Following the upgrade, questions regarding the new PeopleSoft system can be directed to the Corporate Computing Help Desk (505-844-2695) by choosing option “0” (zero).

The PeopleSoft upgrade will be completed in stages to minimize impact on users. The PeopleSoft upgrade is expected to be completed by the end of June.
I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)

I'm the project lead for the Sandia LOIS team. LOIS, by the way, is the LDRI Orbiter Inspection System. LDRI stands for laser dynamic range imager. We use a lot of acronyms in this business, but you get used to them. Our LOIS team has been an integral part of the space shuttle program ever since the Return to Flight mission following the Columbia accident.

Let me give you a little bit of background. You may recall that what destroyed the Columbia was the damage to its thermal protection system — the TPS — when a chunk of foam insulation broke away from the space shuttle's main fuel tank during launch and slammed into the orbiter wing's leading edge at supersonic speeds. The damage compromised the spacecraft's protective skin, allowing the massive heat of re-entry to burn its way into the shuttle's structural framework. Columbia broke up over the southwestern US; pieces were recovered in Texas and Louisiana. All seven members of the crew were killed.

This is where Sandia comes in. We designed and built the LDRI to inspect the TPS for any damage and to move the crew to the ground for analysis. The Sandia team members and their NASA colleagues scrambled for a solution, ultimately developing an approach that got the job done with time to spare.

In this first-person account, written at the request of the Lab News, Sandia project lead Jose Rodriguez conveys a you-are-there sense of urgency to work the problem and help ensure the astronauts got home safely. The team was honored by NASA mission planners for its efforts.

By Jose Rodriguez (2664)
Sandia to play major role in simulation of ‘virtual’ nuclear reactor

By Neal Singer

Sandia computational scientists will lead two of five technical areas in a DOE effort to create a “virtual” nuclear reactor, to be headquartered at Oak Ridge National Laboratory (ORNL).

The advance simulation will use capabilities of the world’s most powerful computers to attempt significant leaps forward in nuclear reactor design, engineering, and operation. Information gleaned from a virtual model of a currently operating reactor could help improve nuclear reactor safety, increase reactor power output, and reduce licensing requirements over the near, mid, and long term.

The work, funded by a DOE award of up to $122 million over five years, will be coordinated from a Nuclear Energy Modeling and Simulation Energy Innovation Hub (Hub), named the Consortium for Advanced Simulation of Light Water Reactors (CASL), includes partners from many national laboratories. CASL is tasked with delivering computer models that simulate nuclear power plant operations. These models will then be incorporated into a computational environment that forms a “virtual reactor” for the predictive simulation of light water reactors (LWRs).

“The next 18 hours went on like this: We would get an AVI file, process it, and then wait four or five hours for the download to complete. A big push for speed-up was working out great. We received the next file in about 10 hours. It was very frustrating. I’ve learned that the file size (6-7 GB per file) was a little large for the space station’s network. Also, the processed data rates weren’t being achieved and file transfers would fail due to loss of satellite coverage. NASA’s Comm and Track team was handling the file delivery for us and I have to credit them with doing all they could, but all of our data couldn’t be downloaded in a single transfer due to the KU antennae not working. In the background, Bob Nellums (5711, standing) and Shawn Ward (NASA) were working out great. We received the next file in about 10 hours. It was very frustrating. I’ve learned that the file size (6-7 GB per file) was a little large for the space station’s network. Also, the processed data rates weren’t being achieved and file transfers would fail due to loss of satellite coverage. NASA’s Comm and Track team was handling the file delivery for us and I have to credit them with doing all they could, but all of our data couldn’t be downloaded in a single transfer due to the KU antennae not working. In the background, Bob Nellums (5711, standing) and Shawn Ward (NASA).

...AIAA and Andy Romero (NASA) hang the STS-131 plaque in the Mission Evaluation Room (MER). The LOIS team and the Comm and Track team were being honored by the NASA plaques for their outstanding contributions during STS-131. We were invited to be part of the STS-131 plaque-hanging ceremony — a tremendous honor and a testament to the expansion of nuclear power and long-term sustainability — for our outstanding contributions during the mission. I was so proud of the moment as I’ve ever been. It was gratifying to me personally that our long hours and hard work had paid off and was recognized in its own way contributed to the overall mission success. On April 20, after being delayed by weather for the day, Discovery landed back where it had begun its mission, at Kennedy Space Center in Florida. The shuttle was in sight in Discovery’s 26 years of service and 38 missions. On that day, on behalf of the entire LOIS team, I helped hang the STS-131 mission plaque in the MER conference room, which is right across the hall from the old Apollo mission control center. What a way to cap off such a challenging mission.
What is an out-of-pocket maximum and how does it work?

Note: This information is provided by Sandia’s Benefits organization. Previous Take Charge Corner articles have addressed other “floors” and features of the Total Health house.

This article completes our tour of the Sandia Total Health house. In the four previous articles we took a close look at biometric screenings and health assessments, health reimbursement accounts, preventive care, and the deductible and coinsurance. We learned how the Sandia Total Health plan design shelters the members from excessive healthcare costs. And, as with any solid structure, most shelter is provided by the roof or ceiling. In the case of Sandia Total Health, that shelter for members comes in the form of the out-of-pocket maximum.

The out-of-pocket maximum is the maximum amount you’ll pay out of your own pocket for in-network eligible medical care during a plan year, including your annual deductible amount. That means any money you pay for in-network eligible expenses to meet the deductible also counts toward your out-of-pocket maximum.

The in-network out-of-pocket maximum is based on the coverage tier you elect. For Sandia Total Health, if you have:

- Employee-only coverage: your out-of-pocket maximum is $2,750 per year
- Employee + Spouse or Child(ren) coverage: your out-of-pocket maximum is $5,500 per year ($2,750 per person)
- Employee + Spouse and Child(ren) coverage: your out-of-pocket maximum is $8,250 per year ($2,750 per person)

Note: These out-of-pocket maximums apply only to in-network care. Out-of-network care has different out-of-pocket maximums. For more information, review your plan comparison chart.

Once you reach the maximum, your remaining in-network eligible expenses for that plan year are covered at 100 percent.

For more information about the Sandia Total Health plan design features, visit the Take Charge website at www.SandiaTakeCharge.com.

The chart below offers an example of how the out-of-pocket maximum works for employee-only coverage.

**Remember:** If you have more than one person under your coverage, the out-of-pocket maximum will work like this for each individual person under the coverage (up to three times the individual maximum).

Meet Bob: Bob (see chart) has employee-only coverage under Sandia Total Health, and used only in-network providers during the year. Bob completed a biometric screening and a health assessment, so Sandia contributed $250 to his Health Reimbursement Account (HRA). Let’s take a look at how Bob’s annual medical services are covered by Sandia Total Health.

### Important facts about the out-of-pocket maximum:

- **If you have Employee + Spouse and/or Child(ren) coverage, each person covered under the plan has an individual out-of-pocket maximum. That means that when one person meets his/her $2,750 maximum, the remaining eligible expenses in that plan year for that individual are covered at 100%.

- **Prescription drug costs are not included in the annual out-of-pocket maximum amounts listed above. There is a separate annual out-of-pocket maximum amount you pay for prescription drugs: $1,500 per person for prescription drugs purchased in-network.

### Chart: Out-of-Pocket Maximum

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost of Service</th>
<th>Description</th>
<th>Claims Processing Amount</th>
<th>Sandia’s Responsibility</th>
<th>Bob’s Responsibility</th>
<th>Bob’s Out-of-Pocket Accumulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Preventive Care</td>
<td>$250</td>
<td>In-Network Preventive Care Covered at 100%</td>
<td>N/A</td>
<td>$250</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Specialist Visit</td>
<td>$250</td>
<td>Health Reimbursement Account (HRA) – $250*</td>
<td>Entire $250 applies to deductible but is reimbursed by HRA</td>
<td>$0</td>
<td>$250**</td>
<td>$250**</td>
</tr>
<tr>
<td>In-Network Deductible –</td>
<td>$750</td>
<td>X-rays</td>
<td>Entire $500 applies to deductible</td>
<td>$0</td>
<td>$500</td>
<td>$750</td>
</tr>
<tr>
<td>$750</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCP visit</td>
<td>$100</td>
<td>In-Network Coinsurance – You pay 20%, up to $2,000</td>
<td>20% coinsurance</td>
<td>$80</td>
<td>$20</td>
<td>$770</td>
</tr>
<tr>
<td>Ambulance</td>
<td>$800</td>
<td></td>
<td>20% coinsurance</td>
<td>$640</td>
<td>$160</td>
<td>$930</td>
</tr>
<tr>
<td>Hospital Stay</td>
<td>$15,000</td>
<td>In-Network Out-of-Pocket Maximum – $2,750</td>
<td>20% coinsurance</td>
<td>$13,180</td>
<td>$1,820</td>
<td>$2,750</td>
</tr>
<tr>
<td>TOTAL</td>
<td>$16,900</td>
<td></td>
<td></td>
<td>$14,150</td>
<td>$2,750**</td>
<td>$2,750**</td>
</tr>
</tbody>
</table>

* Annual HRA contribution amounts are $250, $500, or $750, depending on your coverage tier.
** First $250 of Bob’s eligible expenses is reimbursed by HRA funds, yet still applies toward Bob’s deductible and out-of-pocket maximum. Bob’s actual out-of-pocket amount is therefore $2,500: $2,750–$250 reimbursement from the HRA.
**Feedback**

**Q:** Will the Description field, where each individual can enter his/her own text description for each P/T, continue to be available for timecards in the PeopleSoft 9.0?

A: Individuals are not allowed to enter their own text description for each project and task and were not able to do so in the current system, ETK, either. The project and task that the employee enters is flowing directly from Oracle Financials and is not configurable for any other options in the new timekeeping system. There is a drop-down menu in the new system where allowable project and task data is viewable, but no description for them is identified through the Oracle Financials into the timekeeping module. For further questions/concerns regarding this issue, please contact the payroll helpline at 844-2848.

---

**Recent Retirees**

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Huskisson</td>
<td>39</td>
<td>2555</td>
</tr>
<tr>
<td>Bruce Tuttle</td>
<td>29</td>
<td>1816</td>
</tr>
</tbody>
</table>

---

**PeopleSoft questions answered**

**Q:** How do we account for including our allowable breaks, please call your HR representative for that guidance.

**Q:** Is there a way to set up a profile, as they did in the current system, ETK. What the employee will be able to do is to enter his/her own text description for each P/T, continue to be available for timecards in the PeopleSoft 9.0?

A: Through the new timekeeping system training, ETC100, we identified that employees will not be able to set up a profile, as they did in the current system, ETK. The timekeeping system has not changed with respect to taking classes offered by HBE at lunch time? Some of the classes are 45 minutes long and it is a wonderful benefit that Sandia has provided to the MOW’s.

**Q:** What is this timekeeping change going to affect MOW’s ability to take advantage of the exercise classes offered by HBE at lunch time? Some of the classes are 45 minutes long and it is a wonderful benefit that Sandia has provided to the MOW’s.

A: The timekeeping system has not changed with respect to taking classes offered by HBE during lunch time. Please work with your manager on time charging for attending classes during regular work days. The timekeeping system isn’t a punch clock, it is merely being used to assist in determining proper charging for overtime considerations for our nonexempt workforce.

---

**Mileposts**

New Mexico photos by Michelle Fleming

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cynthia Caton</td>
<td>25</td>
<td>9343</td>
</tr>
<tr>
<td>Harry Caton</td>
<td>25</td>
<td>2113</td>
</tr>
<tr>
<td>Dennis Lierz</td>
<td>25</td>
<td>5335</td>
</tr>
<tr>
<td>Fred Oppel</td>
<td>25</td>
<td>6385</td>
</tr>
<tr>
<td>Michael Partridge</td>
<td>25</td>
<td>2627</td>
</tr>
<tr>
<td>John Torczynski</td>
<td>25</td>
<td>1513</td>
</tr>
<tr>
<td>James Cales</td>
<td>20</td>
<td>12311</td>
</tr>
<tr>
<td>M. Wayne Davis</td>
<td>20</td>
<td>1100</td>
</tr>
<tr>
<td>Kathryn Fortune</td>
<td>20</td>
<td>10541</td>
</tr>
<tr>
<td>Brian Greary</td>
<td>20</td>
<td>2113</td>
</tr>
<tr>
<td>Barbara Jennings</td>
<td>20</td>
<td>9531</td>
</tr>
<tr>
<td>Emily Lujan</td>
<td>20</td>
<td>10659</td>
</tr>
<tr>
<td>John Pameiier</td>
<td>20</td>
<td>6418</td>
</tr>
<tr>
<td>Kent Robbins</td>
<td>20</td>
<td>2542</td>
</tr>
<tr>
<td>Patsy Rowland</td>
<td>20</td>
<td>4825</td>
</tr>
<tr>
<td>Everett Saverino</td>
<td>20</td>
<td>12320</td>
</tr>
<tr>
<td>Martha Bersich</td>
<td>15</td>
<td>10507</td>
</tr>
<tr>
<td>Charles Brady</td>
<td>15</td>
<td>5339</td>
</tr>
<tr>
<td>Richard Field</td>
<td>15</td>
<td>1526</td>
</tr>
<tr>
<td>Michelle Griffith</td>
<td>15</td>
<td>5578</td>
</tr>
<tr>
<td>Marcy Hoover</td>
<td>15</td>
<td>12141</td>
</tr>
<tr>
<td>Charles Rhyleard</td>
<td>15</td>
<td>6418</td>
</tr>
<tr>
<td>Lisa Trainor</td>
<td>15</td>
<td>5096</td>
</tr>
</tbody>
</table>
By Stephanie Hobby

Sidney Gutierrez (4100), former NASA astronaut, retired US Air Force colonel and current director of Environment, Safety, and Health and Emergency Management, was named the 2010 Notable New Mexican by the Albuquerque Museum Foundation. He was honored June 2 at the 10th annual award ceremony, where award-winning santero artist Arthur López unveiled a bulto depicting Sid and the story of his life. A bulto is a three-dimensional traditional New Mexican genre of wood carving.

“This is way beyond my wildest expectations,” Sid said as the bulto was unveiled. “It really takes my breath away, and I hope that young people who come to the museum will be encouraged to learn and explore more.”

The Notable New Mexican award was started as a way to preserve the state’s history and to enhance the museum’s art collection. Every year, the Foundation recognizes an outstanding individual with unique accomplishments and strong ties to the state. Recipients are presented with a commissioned artwork, which is then permanently displayed at the Albuquerque Museum.

“We are so pleased to present this award to such an inspirational figure in the community,” says Debra Ilomero, executive director of the Albuquerque Museum Foundation. “Sid’s life mirrors the history of Albuquerque, from having roots in agriculture to being a central part of the nation’s high-tech industry. We see the opportunity to celebrate Sid as an opportunity to celebrate Albuquerque.”

Sid’s family heritage can be traced back through 300 years of Duke City history, but his family originally descended from people living in the area more than 30,000 years ago.

“My family and I are very excited about the art and this award,” says Sid. “I look at this as what it means to my family and my friends. I look back at my ancestors, and my grandfathers in particular, and what they did to get me to where I am today. I look at my teachers who helped me out. I look at my family and friends who supported me, and I have been so fortunate in that regard. This is a great honor, and I am pleased to share it with those who have supported me over the years.”

Sid was born in 1951, just four years after Chuck Yeager tore through the sound barrier, and six years before a beach-ball sized satellite named Sputnik went up. Like most children who grew up in the height of the US-Soviet space race, Sid was caught up in the fever of space flight and exploring the unknown. He made a commitment to become an astronaut while in fifth grade at Los Ranchos Elementary School. While his peers only dreamed of flying in space, Sid pursued his goal with fierce determination. He contacted NASA to learn the requirements of the astronaut training program and methodically made his way through the rigorous criteria.

Sid was accepted to the US Air Force Academy in 1969, the same year that two American men left the first footprints on the moon. Sid studied aeronautical engineering and was a member of the National Collegiate Championship Parachute team. He did more than 550 jumps, and rose to the ranks of master parachutist. Not surprisingly, Sid’s perseverance led him to graduate at the top of his class. He became a fighter pilot and then a test pilot before being selected by NASA for astronaut training in 1984. On his first trip to space in 1991, he served as the pilot for the space shuttle Columbia, and in 1994 was the commander of the space shuttle Endeavour.

Five months after touching down at Edwards Air Force Base, Sid and his family returned to Albuquerque, where he started work at Sandia. He is currently the director of Environment, Safety, and Health and Emergency Management at Sandia.

“Sid is a great New Mexican and a great patriot,” says Executive VP and Chief Operating Officer Al Romig. “I can think of few others who have done as much in their lifetimes to make this country great. Sid is surely deserving of this award.”

Every year for the past 10 years, the Albuquerque Museum Foundation has presented the Notable New Mexican award to celebrate the accomplishments of an extraordinary New Mexican with strong ties to the state and exemplary service to the public good.

All past award recipients have been presented with a portrait, which is permanently displayed at the Albuquerque Museum. This year, Sid chose to be depicted in a bulto, to reflect his family’s New Mexican heritage. The santero artist, Arthur López, is a native of Santa Fe, and has received numerous awards for his work and exhibits his art at shows throughout the Southwest.

A Notable Family Day event, “The Astronaut and the Artist: Storytelling, Inspiration and Craft” will take place July 10, 1-3 p.m., at the Albuquerque Museum and include presentations from Sid and López. This program is free to the public.

A NOTABLE MAN — Sid Gutierrez reacts to seeing the bulto in his honor at the 2010 Notable New Mexican Gala on June 2. Artist Arthur Lopez is second from right. (Photo by Jean-Paul Jager)

Talented group helps bring talent into Labs

PeopleSoft v9.0 Upgrade Toolkit

It’s almost here . . .

SANDIA LAB NEWS    June 18, 2010    Page 12