Cloudbusting

The "Cloudbuster" was a device invented by William Reich to create clouds and rain by shooting "energy" into the sky through a series of metal rods. Although Reich was paid by many desperate farmers to produce rain, the device was never proven to work.

It's been ten years since the Office of Management and Budget (OMB) released the original Federal Cloud Computing Strategy. I had the opportunity to update this strategy two years ago when I served as the Cloud Policy Lead at OMB. Having spent 20 years in the private sector building bleeding-edge cloud infrastructure for some of the best known companies in the world, I was able to leverage my practical experience in the creation of the 2019 Federal Cloud Computing Strategy, "Cloud Smart".

During the course of my work at OMB, I spoke with hundreds of practitioners, policy experts, and Chief Information Officers (CIOs) across government. From this vantage point, I had an intimate view into the entire Federal technology portfolio and learned that many myths about cloud computing were being accepted as truth.

In this article, I'll debunk key myths about cloud adoption, and explain why - and when - cloud is appropriate for government. These myths are generally intended for civilian Federal agencies of the United States, but the recommendations below apply to any public sector organization - and even some private organizations as well. In part two, I'll discuss some strategies for overcoming the pitfalls discussed here.

Myth 1: Cloud Is Cheaper

The main reason cited by Federal agencies to move to commercial cloud is the promise of cost savings. This myth originated with vendors and was repeated by Congress, eventually becoming a common talking point for Executive Branch agencies. Unfortunately, it is based on false premises and poor cost analyses. In practice, the government almost *never* saves actual money moving to the cloud - though the capabilities they gain from that investment will usually result in a greater *value*.

At a glance, it can appear that moving applications to the cloud may be cheaper than leaving them in a data center. But in most cases, a Federal agency will not see much, if any, cost savings from moving to the cloud. More often than not, they end up spending many times more on cloud than for comparable workloads run in their data center. Experts have known this was a myth for at least a decade, but the lobbyists and salespeople were simply louder than those who had done the math.

First, it's important to note that most Federal agencies own outright the facilities their data centers are located in. In the 1980s and 1990s, agencies began repurposing existing office space for use as data centers, adding in advanced cooling and electrical systems to support their growing compute needs. This changes the equation for the total cost of ownership because the facilities are already built and can be run *relatively* cheaply, though they may be partially or fully staffed by contractors due to the constant push to outsource all work. The government has also built a *few* best-in-breed data centers such as the Social Security Administration's flagship data center that can compete with some of the most efficient commercial facilities in the world, with solar collectors for electricity generation, and advanced heat management systems for reduced energy usage. However, these super-efficient facilities are only represent a handful of the over 1500 data centers the government owns and operates, and cost half a billion dollars each to build.

Second, agencies routinely run their servers and equipment well past the end-of-life to save money. There are no Federal requirements to update hardware. In fact, until recently, Federal data center requirements for efficiency measured the utilization of servers by time spent processing, which *disincentivized* agencies from upgrading - older hardware runs slower and thus results in a higher *utilization* rate for a given task than a newer, more efficient server that completes the task quickly. During a budget shortfall, an agency with a data center has the option of skipping a hardware refresh cycle or cutting staff to make up the deficit; meanwhile, an agency that is all-in on cloud loses this option, as they will have to continue paying for licenses, operations and maintenance costs. As a result, agencies will need to future-proof their plans in more innovative ways, or better communicate funding priorities to OMB and Congress.

Also, it's important to realize that once the government does buy hardware, the government owns it outright. When you move your application to a commercial cloud, you're paying a premium for data storage even if it's just sitting around and not being actively used - for large amounts of data, cloud costs will quickly skyrocket. The government maintains *decades* worth of massive data sets - NASA generates *terabytes* of data per day, and even a tiny agency like the Small Business Administration has to maintain *billions* of scanned loan documents going back to its inception sixty years ago. This is why some major companies have moved away from commercial cloud and built their own infrastructure instead.

I would note that the idea of workload portability - moving a service between different cloud vendors, generally to get a cheaper cost - is also largely a myth. The cost to move between services is simply too great, and the time spent in building this flexibility will not realize any savings. Moreover, every cloud vendor's offering is just *slightly* different from its peers, and if you're only using the most basic offerings which are identical - virtual servers and storage - you're missing out on the full value that cloud offers.

Myth 2: Cloud Requires Fewer Staff

Another promise of cloud cost savings is that an agency no longer has to keep data center engineers on staff. These practitioners are usually comparatively cheap to employ in government, and rarely reach a grade above GS-13 ($76K-$99K annual salary) and agencies moving to cloud will instead employ comparatively expensive DevSecOps practitioners, site reliability engineers, and cloud-software engineers to replace them when moving applications to IaaS or PaaS. These types of staff are extremely difficult to hire into government as they make very high salaries in the private sector, well in excess of the highest end of the General

Schedule pay scale (GS-15: $104K-138K), even assuming an agency has the budget and staff slots open to create a GS-15 position in the first place. Due to the many flaws in the government hiring process, it also can be very difficult to recruit these people into government, even with the new OPM hiring authorities to streamline this process.

An agency that chooses to outsource these skills will often find that contractors may cost even more than hiring capable staff. The agency will still need to have staff with cloud experience to actively manage these staff, and contracts will need to be carefully crafted around concrete outcomes so that the agency is not fleeced by a vendor.

Another overlooked cost here is training. New solutions aren't always easy for agencies to adopt - whether that's a fancy software development tool or something as simple as a video chat platform. Personally, a day doesn't go by that I don't find myself explaining to a customer some aspect of Teams or Sharepoint they don't know how to use. Agencies often must provide formal training, and of course there's inevitably a loss of productivity while teams get up to speed on the new tools and solutions. Since many SaaS vendors roll out new features extremely rapidly, this can present a challenge for slow-to-adapt agencies. Although some training is provided free from vendors, this rarely suffices for all of an agency's needs, so in most cases further training will have to be purchased.

Myth 3: Cloud Is More Secure

A constant refrain is that cloud is safer and more secure, owing to the fact that the servers are patched automatically - meaning that key security updates are installed immediately, rather than waiting for a human to make the time to roll out all of these updates. For a large enterprise, this is historically a very time-consuming manual process, which automation has improved dramatically. However, the same tools that major corporations use for patching in the Cloud are largely open source and free, and they can be used in an agency's own data center.

Moreover, it's important to note that cloud does not remove complexity, it only hides it in places that are harder to see. When it comes to security, this is especially true, as organizations must adapt to highly-specialized security settings that are not always easily found, particularly with the IaaS offerings. These settings are also constantly changing because of the constant-patching of these vendors, and all too often with little notice in the case of SaaS offerings. This "double-edged sword" has resulted in a number of high-profile cloud-related breaches over the last few years - affecting both the public and private sectors alike as we learn best security practices the hard way.

Cloud vendors have also been… less than enthusiastic about meeting government security and policy requirements, unless the government is willing to pay a very high premium for the privilege of security. (I talked about this contentious relationship more in my post on Automation Principles.) For instance, as of today no major cloud vendor completely meets the government requirements for IPv6 which have been around for 15 years and which OMB recently revised to try to get them to move faster.

Myth 4: Cloud Is More Reliable

This one is less of a myth and more of an overpromise, or fundamental misunderstanding of the underlying technology. For a long time, one of the main pitches of cloud is that of self-healing infrastructure - when one server or drive fails, a new one is spun up to replace it. Although this is something that *can* be implemented in the cloud, it's definitely not the default. Specifically, for IaaS solutions, you have to build that into your application - and you don't get it for free.

Relatedly, many agencies assume that any application put into the cloud will automatically scale to meet any demand. If your agency's website gets mentioned by the President, let's say, you wouldn't want it to collapse due to its newfound popularity. Without building infrastructure designed to handle this, simply being "in the cloud" will not solve this problem. However, solving it in the cloud will likely be faster than waiting for physical servers to be purchased, built, shipped, and installed - assuming you have staff on-hand who can handle the tasks.

It is important to keep in mind cloud is, by definition, *ephemeral*. Servers and drives are often replaced with little-to-no notice. I've frequently had virtual machines simply become completely unresponsive, requiring them to be rebooted or rebuilt entirely. When you're building in the cloud, you should assume that anything could break without warning, and you should have recovery procedures in place to handle the situation. Tools like Chaos Monkey can help you test your recovery procedures.

One issue that some of the most seasoned practitioners often miss is that all cloud providers have hard limits on their resources that they are able to sell you. After all, they are just running their own data centers, and there are a fixed number of servers that they have on-hand. I have often encountered these limits in practical, seemingly-simple use cases. For instance, I've created applications which needed high-memory virtual servers, where the provider didn't have enough instances to sell us. During the pandemic response, I also discovered that cloud-based email inboxes have *hardcoded, technical limits* as to the volume of mail they can receive. I had assumed we could simply buy more capacity but this was not the case, requiring a "Rube Goldberg machine" workaround of routing rules to handle the massive increase associated with a national disaster. There is no question that scalability is a huge benefit, *until* the practical limits become a *liability* because of your assumptions.

Myth 5: Cloud Must Be All-or-Nothing

Many organizations assume that the goal is to move everything to a commercial cloud provider. Both the Government Accountability Office and Congress have stated that the government needs to "get out of the data center business." However, this is simply not a realistic goal in the public sector - government couldn't afford to make such a massive move given their very restricted budgets.

We also must clarify the concept of "legacy systems," another frequent talking point. Most Federal agencies that have been around for more than 30 years still have mainframes, and they're often still running older programming languages such as COBOL, Fortran, and Pascal.

Many major industries in the private sector still use these *same technologies* - most notably, the banking industry still is heavily dependent on these legacy systems. Regardless of the hype about cloud and blockchain for moving money around, 95% of credit card transactions still use a COBOL system, probably running on a mainframe behind the scenes. These systems are not going away *any time soon*.

Now these mainframes usually are not dusty old metal boxes that have been taking up an entire basement room for decades. Often, they're cutting edge hardware that's incredibly efficient - and even have all the shiny plastic and glowing lights and advanced cooling systems you'd expect to see on a gamer's desktop computer. Dollar for dollar, modern mainframe systems can be more cost-effective than cloud for comparable workloads over their lifecycle. It's also worth noting that they are about a thousand times *less likely* to be attacked or exploited than cloud-based infrastructure.

The code running on these mainframes, on the other hand, is likely to be *very old*, and it's almost certainly been written such that it cannot be virtualized or moved to the cloud without rewriting partially or entirely at great expense. Modern programming languages come with their own risks, so finding a *sustainable* middle path between the ancient and bleeding-edge is important for a successful modernization effort.

Due to the considerations above, the future of government infrastructure will remain a hybrid, multi-cloud environment - much to the consternation of cloud vendors.

"… I just know that something good is gonna happen"

Instead of these myths, the best reason to use cloud is for the unrivaled *capabilities* that these tools can unlock:

- Agility: being able to quickly spin up a server to try something new is much easier in the cloud, if you have not already created an on-premise virtualized infrastructure. Cloud.gov, an offering from the General Services Administration (GSA) that bundles many Amazon Web Services (AWS) offerings in a government-friendly "procurement wrapper" can make this even easier for agencies.

- Scalability: the main hallmark of cloud is using this agility to quickly respond to sudden increases in requests to websites and applications. Especially during the COVID-19 pandemic, agencies have taken advantage of this functionality to deal with the dramatic increase in traffic to benefit applications and other services. However, it is critical to note that most cloud services do *not* scale automatically (another myth covered below).

- Distributed: most Federal agencies have staff in field offices all over the country, and of course their customers are both at home and abroad. Since the cloud is really just a series of distributed data centers around the world, this can dramatically reduce the latency between the customer and the service. For instance, agencies are using cloud-based virtual private network (VPN) solutions to securely connect their staff to internal networks. Those that have moved to cloud-based email, video chat, and document collaboration tools see an additional speed bump for staying in the same cloud for all of these services.

Of course, we all know that “cloud is just someone else’s data center,” but the government should not be held back by fear, uncertainty, and doubt from someone else holding their data. Cloud technologies have a huge potential to improve Federal technology, when approached with a full knowledge of the complexity and costs.

Cloud is not a replacement for good management, however. You can’t buy your way out of risk. Until the government invests in its workforce to make sure that IT can be planned, acquired, implemented, and maintained effectively, we will not see any improvement in the services provided to the American people. Now, Congress just needs to be convinced to fully fund some of these improvements.

Cloud Strategy Guide

Chapter 1 - Migrate Pragmatically

The first thing to accept is that not all projects are appropriate for the cloud, and not all organizations have the skills necessary to fully take advantage of the cloud. With that as a starting point, an organization needs to come up with a way to rationalize its application portfolio, to determine what should stay on-premises and what should be modernized. As a general rule, "lift-and-shift" - moving an application without rewriting it for the cloud environment - is *almost never cost-effective* for Infrastructure as a Service (IaaS) offerings unless it's already a *very* modern system in the first place. On the other hand, basic websites with mostly static content are ideal for moving into Software as a Service (SaaS) or Platform as a Service (PaaS) offerings.

The CIO Council's Application Rationalization Playbook (disclaimer: another document I worked on) is a useful starting point for this evaluation. Specifically, an agency should work up a thorough analysis of alternatives between various SaaS, PaaS, and IaaS offerings against the existing on-prem setup, or a hybrid environment. A major consideration here will be the Total Cost of Ownership (TCO), which should take into account not just service costs, but also staffing, support, and training costs. However, the lowest priced option may not always be the best choice (as I'll be covering below).

Cloud.gov, is an offering from the General Services Administration (GSA) that bundles several Amazon Web Services (AWS) offerings in a government-friendly "procurement wrapper" can make migration even easier for agencies. It's an excellent platform for small agencies, or for large agencies that just want to prototype a new concept quickly.

When you do start moving applications, it's important to start tagging your assets - accounts, virtual machines, workflows, etc. - as early as possible to make accounting easier. Always include the project name and the customer organization at a minimum. Some providers also allow you to easily isolate a project or office's services into a resource group, and this can also simplify this process. This is very important to allow easy payback or showback of funds, but for these models remember to include in these costs the TCO aspects not captured - e.g. staff time and contractor resources.

I strongly recommend agencies take a very *cynical* stance on so-called low-code/no-code platforms, customer-relationship management tools (CRMs), and workflow management solutions. Many of you may remember the promises of "Business Intelligence" solutions in decades past, where agencies were fleeced for billions of dollars in configuration costs - these solutions are simply using a new buzzword for the same idea. These all promise to reduce costs but are often vastly more expensive than just building a tool from scratch - and the agency becomes *completely* locked-in to a single vendor until they replace the application entirely. The brilliant Sean Boots of the Canadian Digital Service has presented a "1-day rule" to help identify these boondoggles.

Checklist	
⚖	Rationalize the application portfolio
🚫	Don’t lift-and-shift
☁	Use cloud.gov
🏷	Properly tag cloud assets
🚫	Avoid low-code/no-code/crm snake oil

Chapter 2 - Plan to Your Budget & Staff

The easiest way to avoid risks and unexpected costs is to simplify as much as possible. Civilian agencies should not be investing in bleeding-edge technology solutions - they’re too risky and expensive to maintain. Instead, pick the simplest possible solution that can be supported by your staff. The average agency should be aiming to stay well behind the “hype curve” into the “plateau of productivity.” Since most of the complexity is hidden from the customer, SaaS and commercial-off-the-shelf (COTS) tools are less risky than PaaS and IaaS options overall (provided you follow the 1-day rule above). This goes beyond just cloud, and applies to most anything you’re *building*. Most agencies, for instance, also should absolutely not be attempting to build a fancy React/Redux/GraphQL single-page application when a plain Wordpress or Drupal website with a few plugins will fulfill the customer’s needs. Building native mobile applications should be *completely avoided* by most organizations as these can cost millions of dollars a year just for upkeep - instead they should build mobile-friendly, responsive websites. Any custom application or tool may not be a sustainable solution given the high complexity and cost of engineers. This also means that agencies should be simplifying their *requirements* to the minimum necessary when comparing alternatives, not just the software itself. Avoiding “one-off” projects and special requests will save massive amounts of time and money.

Instead, agencies must be actively investing in *their staff*. Agencies should allocate two to three times the standard training budget for IT and technology-adjacent staff, including project managers, program managers, and acquisition professionals. Some vendors provide a limited amount complementary training, but inevitably agencies need more than these free offerings. This training should include non-IT topics as well, including diversity awareness training, accessibility, plain language writing, project management, agile development techniques, and budgeting and procurement. GSA offers a variety of programs covering many of these areas.

This must also include hands-on training - sitting through a webinar is no replacement for actual practical engineering experience. These staff need to be given the time and flexibility to practice these skills to develop them - building small test projects and trying out tools. The best teams are constantly changing and learning, so setting aside up to 10% or more of the staff’s time just for practice is not unreasonable - some private sector companies set aside 20%. All of these investments will pay off richly for agencies. Also, make sure your staff is cross-trained and able to fill gaps as they occur.

As your staff begins to understand the new cloud paradigms, it will be important to modify your existing processes to handle the agility the cloud brings. Instead of slow, end-to-end, waterfall process “monorails”, set operational parameters as “guiderails.” Your acquisition process should be modified so that cloud can be purchased like a utility. You should not need to have a Change Control Board meeting anytime someone wants to create, resize, or destroy a virtual server. Plan a cost range that the entire project will fit within and review as needs change, along with monthly or quarterly portfolio reviews to stay on top of the budget. Instead of codified “gold disk” server images maintained by your team, consider template security rules.

Checklist	
🚲	Simplify the requirements and architecture
📵	No mobile apps, avoid single-page webapps
🧑‍🎓	Train and cross-train your staff
📻	Allocate time for personal development
🚆	Update processes to set guardrails instead of monorails

Chapter 3 - Embrace New Security Models

Agencies must be able to manage the security of everything they run. Going back to the previous strategy, an agency should not deploy anything it cannot manage, and that goes for security as well. This is equally true in on-premises environments, but new operating models require new security models. Both your operations and security teams will need to be familiar with just about every setting that can be changed in your cloud environment - and how to lock them down to prevent exploitation.

Organizations should no longer assume that a solution is secure just because they did an up-front initial review. The Federal government uses a security review process for services and applications known as the Authorization (or Authority) To Operate (ATO), but the implementation varies from agency to agency. Traditionally this is a series of standard security controls that are reviewed, checklist-style, by an agency once every three years. However, agencies that have excelled at cloud security have moved to Continuous Authorization, using monitoring tools to actively verify that the security controls are being met and maintained, twenty-four hours a day and seven days a week.

However, these monitoring checks still must evolve with the products being monitored to make sure new vulnerabilities have not appeared outside the scope of existing checks. As per usual with cybersecurity, vigilance is key. Since attackers are constantly evolving their methods, tools that *automate security responses* as well should be used whenever practical - especially built-in, native from the large vendors that are constantly evolving to meet these threats.

To help combat this second issue, the Federal government has been moving away from so-called "castle-and-moat" perimeter-based security methods which only monitor network traffic. Instead, an approach known as Zero Trust has appeared, taking a data-first methodology of protecting systems instead of *just* the perimeter, verifying user identities in real-time, and allowing staff to only have access to the minimum amount of information necessary to fulfill the task at hand. In this way, when the perimeter is *inevitably* breached, the data assets contained within are still secure.

It also should go without saying that teams should be using multi-factor authentication on all privileged accounts. Whether developers or administrators, using more than just a username and password will dramatically reduce the risk of exploitation. The Federal government has "PIV cards" that are generally used on most devices, but if the vendor does not support them, implementing a token system via any of the commercially-available platforms is fine: Google Authenticator, 1Password, Microsoft Authenticator, and YubiKey are all worth looking at. However, organizations should completely avoid text-message codes sent to phones, as these are easily intercepted.

For public customers that will need to login or prove their identies, all U.S. government agencies should be using Login.gov.

Checklist	
🔘	Research all product configuration settings
🔭	Implement continuous monitoring, not just compliance
⚙	Use security automation tools
☝	Leverage zero-trust practices to protect your data
🪪	Use MFA & Login.gov

Chapter 4 - Understand What You're Buying

Cloud isn't going to make your teeth whiter or your breath fresher or fix all of your problems, regardless of what the salespeople tell you. You need to know *exactly* what you're buying. Before making an investment, make sure you fully understand what capabilities you're purchasing and what parts you - and the vendor - will be responsible for.

If your evaluation team does not have technical expertise, bring engineers into the conversation early, to sort the truth from the sales pitch. As discussed in the previous article, you may not be getting autoscaling or load balancing or other features you've assumed just happen "automatically" - and if available these features definitely will not be free. You may have to build more "glue" between services than you assume, and someone will have to maintain this connective tissue.

Also keep in mind that the government cloud regions (or "govcloud" by some vendors' naming) provide different versions of these tools than the commercial ones. As a result, not all features or solutions will be available - so again, plan ahead. Though, in most cases, civilian agencies not dealing with highly-sensitive data should consider using the commercial versions whenever possible - the security differences are not so great as to be insurmountable, but the functionality limitations are huge.

Before implementing a service, do careful research on the service limits - maximum traffic or number of virtual machines or emails that can be sent, etc.. Do *not* just trust what you are told by a vendor's engineers or customer representatives - most of the time, they also do not know about these limits until you run aground on them. You should estimate your expected usage - number of site visits and/or users and/or emails, etc., and actually spend the time to search through user forums to make sure no one has hit a limit related to what you're doing.

Customer Experience (CX) is another area where the private sector has been building people-friendly interfaces into their SaaS solutions, and agencies can skip a lot of the hard work and directly benefit from the results. Metrics and feedback-loops are often built-in as well. Maximizing these built-in elements can radically improve an agency's public satisfaction scores at little or no additional cost.

Checklist	
♛♟	Validate assumptions; know your responsibilities
🚪	Consider commercial cloud instead of govcloud
🦄	Research service limits in advance
💬	Leverage built-in CX tools

Chapter 5 - Build a Family Farm

Given that agency IT budgets continue to be cut, and staffing has not increased in 40 years, agencies are largely unprepared to completely rewrite and replace all of their legacy systems. Moreover, "IT Modernization" as a concept is an unending pursuit, as in Zeno's paradox of Achilles chasing the Tortoise, software written today is legacy tomorrow. Agencies will need to use all available funding sources to overcome their deep technical debt, prioritizing those that present the *greatest risk*: those that are unmaintained, frequently used by customers, and lacking in resilience and redundancy. Under this scrutiny, agencies may find that their public websites are a bigger risk than older backend systems.

Also, rather than replacing entire large monolithic systems, they should pull off pieces and replace them independently as resources are available. This can be done by isolating functions and building microservices, but that approach can often lead to expensive, unnecessary complexity. Agencies should not be afraid to build a newer parallel monolith adjacent to the existing one - again, keep in mind that it's not the size that's the concern, but the complexity and sustainability.

That all being said, the government does have major shortcomings in redundancy today, and too many systems have a single point of failure. At a minimum, agencies should be using cloud for data backup of critical systems whenever possible. I also strongly recommend agencies consider creating load balancing and caching layers in the cloud in front of on-premise public-facing systems to deal with unexpected loads.

One final concern is automation. Many organizations begin their cloud journey with unrealistic goals for maturity. The practice of Infrastructure as Code is incredibly popular at the moment, where we talk about treating virtual servers as "cattle, not pets." An unprepared agency may immediately think that they need to be using all of the most cutting edge tools and technologies at first, but this would be a critical mistake. Instead, following the principles relating to complexity in the sections above, agencies should aim to create a "family farm" - only automating that which they can realistically manage. For instance, there is absolutely nothing wrong with only using a few virtual machines and load balancers instead of a fully configuration-only architecture. The great thing about cloud is you can evolve as your team grows, but it's incredibly difficult to reduce complexity you've invested in if your team shrinks.

Checklist	
⚠	Assess technical debt by risk
✂	Replace monoliths a piece at a time
🚫	Don’t over-automate
📋	Use cloud backups and load balancing as soon as possible
🚜	Build a small “family farm” to start

Epilogue - Getting More Help

These strategies are a starting point towards a successful cloud rollout. If you run into trouble, want to talk shop with your peers, or would like to share your own strategies and experiences, there are several communities to engage with:

- The Federal CIO Council Cloud and Infrastructure Community of Practice is the main Federal group for discussing these topics. However, they are currently in the process of changing their charter to allow any U.S. government staff to participate: Federal, state, and local. Membership is free.

- The ATARC Cloud and Infrastructure Working Group is free and open to any government staff, though private sector companies must pay to be members.

- Cloud & Coffee (presented by ATARC & MorphWorks) is a biweekly podcast hosted by myself and Chris Oglesby. Each episode, we chat with a guest about their personal experience with technology modernization, and there’s a live Q&A open during the chat. Any ATARC member can participate; old episodes are publicly available on Spotify.

ITS A SECRET TO EVERYBODY

This website is part of the **Civic Tech Webring**.

- ← Hunter Owens

- Zagaja.com →

Powered by Jekyll