GOING DIGITAL:
A PLAYBOOK
FOR LEGISLATURES

TABLE OF CONTENTS

About the International Republican Institute (IRI)

IRI is one of the world's leading international democracy development organizations. The nonpartisan, nongovernmental institute has supported civil society organizations, journalists, democratic governments, and other democratic actors in more than 100 countries since 1983—in Africa, Asia, Eurasia, Europe, Latin America and the Caribbean, and the Middle East, and North Africa—and currently has offices in 50 countries worldwide. The Technology and Democracy team at IRI works in every region of the world to help grassroots actors turn digitization and the technological revolution into a force for democratic progress.

DO YOU SEE A WAY TO MAKE THIS PLAYBOOK BETTER?

Are there new technologies or needs we should address?

We want your feedback.

Please share your ideas, feedback, comments and requests by emailing Amanda Zink at **azink@iri.org** so we can continue to improve this resource.

Please also visit the living version of this document housed on Gitbook using **https://international-republican-institu.gitbook.io/going-virtual-a-guide-for-parliaments-1**, which is more frequently updated to reflect changes in the digital environment.

WHY THIS MATTERS AND WHO WE ARE

As COVID-19 spread across all regions of the globe over the past year, the entities most needed to respond to this unprecedented crisis — governments and their legislatures — struggled to find ways to continue operations. With economies, societies and citizens all deeply impacted by the continued spread of the virus, it became key for governments and legislatures to find ways to continue to efficiently and transparently operate in a safe manner during this public health crisis, and to be prepared to do so as needed in the future.

For legislatures, continuing to operate safely during the COVID-19 pandemic and during future disruptive crises is paramount not only to the health and safety of the legislature and constituents, but also to democratic integrity. Democratic representation, oversight of the executive branches of government and swift action informed by careful deliberation of legislation are even more critical in times of crisis. A number of executive branches responded to COVID-19 by passing sweeping emergency orders that centralize power, undermine checks and balances and threaten civil liberties; these actions remain in place even as the crises abates. Delayed elections, increased surveillance and restricted freedom of assembly and speech passed as measures to protect public health while further threatening the integrity of global democracies. Well-functioning, strong legislatures – at both the national and subnational level – are one of the first lines of defense against measures that could have lasting negative implications for democracy, digital rights and freedom. The near standstill in legislative operations spurred by the COVID-19 pandemic has further highlighted the critical need for legislatures to modernize and digitize operations — not just in response to crises, but to provide badly needed reinforcement for legislative operations and to advance governance into the modern age.

This toolkit is designed to not only guide legislatures seeking to replicate core functions safely and efficiently online when normal operations have been disrupted, but

■ The near standstill in legislative operations spurred by the COVID-19 pandemic has further highlighted the critical need for legislatures to modernize and digitize operations — not just in response to crises, but to provide badly needed reinforcement for legislative operations and to advance governance into the modern age.

also for those looking to increasingly incorporate digital operations in their everyday legislative business. Many legislatures at both the national and subnational level, have been obliged to turn to digital tools and tactics to overcome newfound challenges and rapidly transition toward a more digitally-forward future. Efforts during COVID-19 have shown that shifting even a few operations online offers legislatures the opportunity to increase governmental accountability, transparency and direct communication with citizens by employing digital tools already in existence. We hope this toolkit will be helpful helpful for subnational and national legislatures, as well as municipal and local councils, to inform, sustain and perhaps build upon increased digital operations beyond the COVID-19 crisis. Many of the tools and resources detailed in this document can help legislatures operate in ways that are more inclusive, efficient, cost-effective and transparent even as normal functioning resumes, or in the face of future disruptive crises.

The first section of this toolkit includes guidance on how to adjust rules and procedures to allow for virtual operations, as well as points to consider in selecting software, hardware and infrastructure. The following sections walk through the core functions of a legislature and provide guidance on how they might be transitioned online, supported by case-study examples and suggested tools that might be used to augment or replace in-person activity. The final portion of this toolkit is dedicated to best practices and methods a legislator or staffer may use to communicate with constituents digitally — not only in times of crisis but as a way to augment and improve upon traditional methods of communication.

Given the continued rapid technological and democratic innovation we are seeing around the world in response to the crisis, a living, collaborative version of this playbook has been developed to allow for reader comments and feedback, accessible here on Gitbook. The document is maintained by the International Republican Institute (IRI), a nonprofit, nonpartisan democracy-development organization with offices in 45 countries, and programs in more than 90 countries. We ask the broader technology and democracy community to share suggestions on the content, point us to relevant tools and share case studies or best practices from around the world.

■ **Efforts during COVID-19 have shown that shifting even a few operations online offers legislatures the opportunity to increase governmental accountability, transparency and direct communication with citizens by employing digital tools already in existence.**

ADJUSTING RULES AND PROCEDURES

To successfully continue core legislative functions — namely electoral representation, drafting and enacting legislation, constituent engagement, authorization of budgets, and oversight — during a disruptive crisis, rapid and coordinated action must be taken. Rules and regulations may need to be adjusted to allow for a continuation of legislative services online. New platforms will need to be used to facilitate continued operations. Information sharing will need to be amplified and acutely verified, not only internally, but also externally with constituents. The following sections will provide guidance, case-study examples and an overview of available tools to help you prioritize as you digitally adapt.

Many legislatures have standing rules and procedures that prohibit virtual operations — sometimes intentionally, but often incidentally. You will need to review laws, rules and — if applicable — the constitution, to identify provisions that may either facilitate or derail all or some aspects of moving parliamentary[1] work online.

> ▶ **The contingency plans developed by the highly digitized government of Estonia have often been considered as the gold standard for digital preparedness.** Its Emergency Preparedness Act, passed in 2000, has provided Estonia with the flexibility and guidance needed to navigate crises that may disrupt digital or in-person operations at both the national and local levels.

PROVISIONS TO LOOK FOR:

- Existing continuity of government (COG) authorization (i.e., defined procedures that allow a government to continue its essential operations in case of a catastrophe, disruption or state of emergency).

- Determine under what circumstances your COG authorization applies. Many COG provisions are delimited to specific emergency scenarios, such as "in case of enemy attack." This language may need to be adjusted to include other crises or standard operating scenarios more broadly.

- Whether the seat of government can be changed and under what circumstances.

- Quorum requirements, and procedures designed to change or suspend those requirements.

- Whether legislative sessions are required to be open.

- Determine whether the legislature may meet remotely — either fully remotely or in a mixed-session format — and if there are unique limitations for plenary, committees, caucuses, etc.

- Determine procedures, provisions and limitations for voting.

- Determine limitations to accessing classified information remotely.

---

[1] Throughout this document, the terms "legislative/parliamentary" and "legislature/parliament" are used interchangeably, both referencing a deliberative assembly with the authority to make laws.

If necessary, the legislature may need to adopt new resolutions to allow for remote deliberation and voting under the auspices of a COG authorization.

New resolutions and updated procedures that allow for virtual operations have been adopted in numerous legislatures across the world in response to the spread of COVID-19, examples of which are linked below. Elements of this language can be adopted to temporarily address COVID-19, to permanently adjust a legislature's operations or in preparation in the case of future crises. Keep in mind that as legal language and the associated processes are adapted for increased digital operations, increased cybersecurity risks and threats must be kept at the forefront of the legislature's discussion (see page 14).

VOTING REGULATIONS:

The **Arkansas** legislature passed legislation to create a temporary emergency procedure to allow voting by limited-directed proxy, providing the authority to cast a vote on behalf of another but only as directed on specific, limited issues.

REMOTE PARTICIPATION:

Legislation was passed in **California** to amend standing rules to allow for remote participation in meetings during emergencies.

In **Brazil**, the legislative work of the Chamber of Deputies is being carried out electronically as much as possible during the pandemic. Legislation has been passed to permit the creation and use of a remote-deliberation system to allow for virtual discussion and voting.

Ecuador passed comprehensive legislation to govern the remote participation in and implementation of virtual sessions, facilitating the use of information and communication technologies (ICTs) to facilitate remote work with parliamentarians and staff, live streaming of plenary sessions and remote voting.

COMMITTEE REGULATIONS:

The **Illinois** legislature passed legislation to allow the president of the legislature, in consultation with the minority leader, to establish the process by which senators and members of the public remotely participate in hearings.

BROAD AMENDMENTS TO RULES DURING EMERGENCIES:

The **North Carolina** legislature passed a resolution to extensively amend the rules and procedures during an emergency, including rules governing the opening of a session, designated voting and the introduction of bills and resolutions.

The **New York** legislature passed a resolution encompassing changes regarding remote participation and remote voting.

In **New Zealand,** sweeping procedures were adopted in the House allowing:

- Adjustment of the limit on the number of votes that may be cast by a proxy holder (someone authorized to vote on another's behalf).

- Oral questions to be logged electronically.

- Select committees to conduct meetings and other forms of decision-making electronically.

The **U.S. House of Representatives** passed H.R. 965, which amended rules to provide for proxy voting and remote committee proceedings.

The **Congress of Chile** adopted a constitutional reform that allows it to hold sessions virtually under exceptional circumstances, parliamentarians to vote remotely and sessions to continue to be livestreamed.

Additional guidance and examples of adjustments to legal and constitutional language in response to COVID, specifically among European Parliament member countries, can be reviewed in the briefing, States of Emergency in Response to the Coronavirus Crisis: Situation in Certain Member States. Further examples can also be found in the Continuity of Legislative Activities during Emergency Situations, providing examples of adjustments legislatures across the globe initially made to either adjust existing legal language or determine methods to adjust legislative procedures within existing legal constraints. See page 21 for a case study in how IRI supported the National Assembly of Armenia in adjusting procedures to operate online within existing legal parameters.

Keep in mind that there are a few processes that would be very difficult to transition digitally. Implementing procedures for the remote access and handling of classified information, for example, would be incredibly difficult and costly to implement.

In the U.S. Congress, for example, members and staff are only able to view and discuss classified information in the Sensitive Compartmentalized Information Facility, or SCIF, which houses secure rooms that prevent outside surveillance or spying. Members and staff cannot email classified information or use encrypted applications like WhatsApp or Signal to share classified information. Given these requirements and the prohibitively long timeframes and high costs of building offsite SCIFs, U.S. congressional committees and staff considering classified information have had to perform their duties onsite. Other legislatures likely have similar constraints in accessing classified information and would need to continue to view and discuss classified information in the legislature's secure onsite spaces. Constraints and challenges such as this should be kept in mind as legislatures consider shifting operations virtually.

SETTING UP SOFTWARE, HARDWARE AND INFRASTRUCTURE

As your legislature begins to review and adjust rules and procedures, it is critical to begin considering the software and internal infrastructure that will make digital operations possible. In order to securely and efficiently move operations online, legislatures will need to ensure that all members and staff have secure, fast access to key software, central file storage and collaboration tools. There are three components to this: software (e.g. word processors and spreadsheets), hardware (e.g. computers, modems and Wi-Fi routers), and infrastructure (e.g. an internet connection). In order to effectively facilitate virtual operations, parliaments need to consider all three.

It is important to keep in mind that all members and staff will require knowledge and skills to be able to successfully use and benefit from these resources, and may require training in order to adequately do so. Investing in conducting trainings — as well as investing financial resources to modernize needed software, hardware and infrastructure — may be required, but these updates will help legislatures advance on the path to greater transparency, accountability, citizen participation and access to information.

🔒 CYBERSECURITY CONSIDERATIONS

Moving legislative operations online inevitably results in increased exposure to cybersecurity threats. **Ensuring cybersecurity has three main components: the architecture of the information systems, user awareness and established policies.[2]** Creating an institutional culture that values security is a critical place to start; this begins with leadership and includes everyone in the organization (see page 14 for best practices and available cybersecurity resources). An excellent place to start is a thorough risk assessment — a deep look into what information and processes are most important to the legislature, what resources are most enticing to its adversaries and the most dangerous vectors of attack. The tailored mitigation strategies that come out of this can help an organization assess the most likely and most high-impact threats, and then channel scarce resources of time, money and people accordingly. If not yet established, legislatures need to consider creating some internal authority that sets policy and monitors information systems and their integrity — as well as conducting cybersecurity training programs and awareness campaigns — to ensure cybersecurity as operations shift online. If the legislature does not have the capability to monitor information-technology (IT) systems in house, consider outsourcing the task to a trusted external partner.

Critical cybersecurity considerations include the development of secure data-communications channels both outside the parliament and among individuals within parliament, the protection of the internal network, the monitoring of parliamentary technology infrastructure, cybersecurity incident response, policy development and review. Before rearchitecting the parliament's online infrastructure, it is highly recommended for legislatures to put in place a detailed program that includes trusted purchase partners for hardware and software, extensive training and ongoing reminders for users, policies with appropriate enforcement and the installation of modern software that is consistently updated and patched.

Contingency plans for digital compromises must also be considered. Estonia's 2018 Cybersecurity Act offers a strong example of the considerations, definitions and obligations that should be addressed before any software, hardware or online infrastructure is put into place. Please see page 14 for an overview of basic best practices an individual can take to ensure cybersecurity.

---

[2] "Fact Sheet: Cyber Security." e-estonia, e-estonia.com/wp-content/uploads/cyber-security-factsheet-aug2020.pdf.

Software

Although there are variances between parliaments on how member offices are provided technical assistance, most parliaments offer some form of support. For the sake of security, cost-efficiency, interoperability and technical support, it is best if a single, centrally administered office suite is deployed for the entire legislature.

QUICK TIPS

- Use a cloud-based office suite — they are more secure, facilitate easier remote collaboration and don't require in-person maintenance. The "cloud" is a centrally maintained set of servers that can be accessed over the internet (see page 14).

- The two most commonly used office suites are Microsoft's Office 365 and Google's G-Suite. Both offer special support and features for democratic actors and governments.

- Consider internet connectivity for staff and parliamentarians. How fast are internet speeds? How much work will be conducted via smartphone or tablet, as opposed to a laptop or desktop computer? While some office suites are entirely based online, others can operate while offline but require a connection to the internet to upload and download files. Select your communication platforms accordingly, and consider diverting funds for internet service upgrades, if possible.

Rules about organizational infrastructure and file storage vary, but a good rule of thumb is that any document stored in a parliamentary office's designated storage site — be that a private server or a smaller drive — remains private even if those files are managed and protected by the parliament at large. For example, the U.S. Congress provides Microsoft email and storage software to its member offices. It does not infringe on the privacy of those emails and documents unless that member's office is under investigation. Parliaments have instituted myriad software systems to facilitate remote file sharing; a few examples include the National Assembly of Ecuador's digital desk software "Curul Electronica," the Chamber of Deputies of Brazil's mobile application "InfoLeg," and the Chilean Chamber of Deputies' digital desk software "Pupitre Electronico," among others.

For a number of parliaments, the COVID crisis has emphasized the importance of digitizing parliamentary documents to begin with. Some parliaments have responded to this challenge by assessing available funds to invest in creating a dedicated IT team and software to facilitate the digitization of documents. If funding is a limitation, however, cloud storage may serve as a viable, lower-cost option requiring little hardware to allow storing and managing digital documents online (see this case study by the U.K. Parliament on using public cloud storage as part of its digital-preservation infrastructure). Regardless of the adjustments made, it is important to consider the longevity of methods selected to digitize parliamentary resources; any digital software or broader infrastructure put in place will have to be actively updated and maintained. This Digital Preservation Strategy developed by the U.K. Parliament in 2008 outlines many of the considerations to keep in mind as materials are digitized.

File Architecture and Access Permissions

Lay out a clear, logical and easy-to-understand file storage architecture as you roll out your office suite. Where will administrative documents be stored? How will your system distinguish between parliament-wide files and collaboration, committees files, party-caucus files and files for specific member offices? Unless noted, allow all permanent staff, except for interns and other temporary staff, access to these folders. Before doing so, invest the time to train staff on file-storage structure and cybersecurity basics to protect your office and legislature (see page 14). The below provides recommendations for the digital file-storage structure for an individual legislator's office:

Parliament administration.
- Human-resource policies (locked for editing).
- IT policies (locked for editing).
- Rules of the parliament.

Office administration (restrict permissions to chief of staff, administrator and member).
- Office budget.
- Employee files and office-specific human-resources policies.
- Office IT policies.

Issues/policy positions.
- Create subfolders for each issue set that house documents describing the member's policy positions in detail.

Constituent correspondence.
- Member letters for constituents (subfolders for each issue set; folders for current and past letters).
- Letters from constituents to the member (subfolders for each issue set; folders for current and past letters).
- Records of constituent phone calls to the member.

Legislation.
- Draft bills, current session
- Final bills introduced, current session
- Final bills adopted, current session
- Amendments introduced, current session
- Amendments adopted, current session
- Resolutions introduced, current session
- Resolutions adopted, current session
- Memorial past sessions (create subfolders for each past session)
- Final bills introduced, past sessions
- Final bills adopted, past sessions
- Amendments introduced, past sessions
- Amendments adopted, past sessions
- Resolutions introduced, past sessions
- Resolutions adopted, past sessions

Letters and official correspondence.
- Letters and official correspondence, current session.
- Letters and official correspondence, past sessions.

Press.
- Press releases, current session.
- Press releases, past sessions.
- Op-eds, current session.
- Op-eds, past sessions.

Constituent meetings.
- Create subfolders for meetings that occur within each issue set, with one each for current session and past sessions — staff would include notes on important constituent meetings with actions taken and their outcomes.
- Other subfolders could be created for important constituent groups, with subfolders created for current and past sessions.

Committees and subcommittees (create subfolders for each committee on which the member sits).
- Committee rules and administration.
- Business meeting agendas, results of legislation considered, copies of legislation considered, notes (subfolders for each business meeting).
- Hearing committee memos, personal office memos, hearing questions, witness testimony, questions for the record (questions submitted to administration officials to answer on the record following the hearing), notes.
- Committee letters and official correspondence, current session.
- Committee letters and official correspondence, past sessions.
- Committee reports, current session.
- Committee reports, past sessions.
- Committee investigations of the executive, current session.
- Committee investigations of the executive, past sessions.

Votes.
- Votes taken in the current session, categorized by issue area and bill.
- Votes taken in past sessions, categorized by issue area and bill.

For all folders and subfolders, be intentional about permissions. Carefully consider who in the office has administrator rights and who has access to which folders. Take additional care to protect static files such as parliament procedures, human-resources (HR) policies or adopted resolutions, locked against editing to ensure no accidental changes are made.

Finally, make sure staff and members keep parliament work, campaign work and personal activity separate, and only use the parliament's office suite for parliamentary activity to avoid confusion, misplacement or misuse of the office organizational structure and record keeping.

It should be recognized that legislatures currently organizing their file architecture fully on paper may face significant barriers to transitioning file storage and management online; personnel-managing offices or departments may not have the capacity or skills to transition to a digital architecture. For guidance and available resources on first steps toward file digitization, visit Preserving Legislative Digital Records, a site created by the U.S. National Conference of State Legislatures aggregating existing tools and examples that may be a helpful resource. Examples of small and large efforts by U.S. states to digitize elements of the existing paper infrastructure can be found at Paperless Efforts in State Legislatures and Authenticating Electronic Documents.

Hardware

There are two general approaches to ensuring access to hardware:

1. Hardware issued by the parliament itself or a member's office. This may include a laptop, mobile phone and other accessories that lead to greater work efficiency. This is the most equitable and secure solution.

2. Bring your own device (BYOD). This policy can range from zero financial support to a capped

amount of support. While this is the cheapest, easiest and most convenient way of approaching hardware distribution — particularly in crises in which the alternative is not possible — it does come with some security concerns, as a single attack could compromise the integrity of the entire system. If this model is chosen, it is especially important to conduct continuous cybersecurity awareness raising for all staff, and systems should be constantly monitored for potential breaches.

Internet Access

It is critical that members and staff have access to the internet both within and outside of the legislature — access to secure computers, a modem to connect to the internet and a router to connect devices to one another should be considered within each member office, in addition to member and staff homes. Consider stipends for home internet connections and associated hardware or, if connectivity is an issue, mobile data can serve as a functional alternative for some core functions. Hotspotting by way of mobile data may provide a faster and cheaper alternative if wired connections are unreliable or more expensive. If mobile data is used to hotspot, keep strong cybersecurity practices in mind, as hotspotting can introduce additional threats (see page 14).

Some countries with poor internet connectivity have created regional offices equipped with reliable internet access and secure hardware to serve as technical hubs for members and their staffers. The National Assembly of Panama, for example, has established and made use of three regional hubs to serve members and staff in rural constituencies. This approach may serve as a lower-cost option that still provides strong internet and telecommunication capabilities near rural constituencies, while avoiding the cost of providing each individual member of parliament (MP) and staffer with reliable Wi-Fi and hardware.

CYBERSECURITY

As governments and their legislatures attempt to respond efficiently and transparently to the COVID-19 crisis, malicious actors have increased their efforts to capitalize on the chaos and sow greater confusion and distrust in governments and their institutions alike. Hacking, disinformation and website takedowns can result in the deception and misdirection of citizens at a moment when clear communications and facts can be the difference between protecting public health or further disrupting it.

As such, the mechanisms your legislature has in place for protecting and maintaining communication channels are more important than ever. This section will highlight the top five actions you can take to secure your legislature, in addition to outlining some of the technical resources that can help you best protect your legislative operations, especially in the case that operations are increasingly shifted online.

Top five actions to protect operations:

1. **Use two-factor authentication (2FA):** Institute a requirement for two-factor authentication to be enabled in order to add a second layer of protection to all important accounts, including to office suites, any email or storage services, and to the social media accounts of all legislators and staff. Use a mobile app or physical key for your second factor, rather than text messaging. For your passwords, use a long series of words or a long phrase; avoid anything short in length. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short with many symbols.

2. **Use a password manager:** Never repeat passwords. Using a password manager such as LastPass, 1Password or Dashlane can help

you keep track of unique passwords for multiple accounts; free or paid versions are available, but be sure to research reliability before use. Password managers such as these can allow you to randomly generate strong passwords and easily track previously used passwords to avoid duplication.

3. **Use the cloud:** A commercial cloud service will be much more secure than anything that you can set up on an individual or office server. Cloud services provide secure management and access information stored remotely on the internet, providing an extra layer of backup if an individual device is compromised and data are lost. Using a cloud-based office suite such as G Suite or Microsoft 365 provides secure email communication, document creation, chat and file sharing; free and more advanced paid versions are available. Even if using a cloud service, be sure to take appropriate steps to secure your computers and phones, such as locking them with a password, keeping your operating system updated, and enabling full-disk encryption.

4. **Use encrypted messaging for sensitive communications:** Encryption is a way of encoding data so that information traveling between users or in storage cannot be read by anyone but the intended recipient. Use encrypted messaging services such as Signal or Wickr for messages, document sharing and phone calls so that, even if a malign actor hacks your device, the messages are protected and unreadable.

5. **Create a culture of safety:** Take cybersecurity seriously, set a strong example and invest the time to train staff. Have a plan if your security is compromised; know who to contact for technical support, understand your legal obligations and have a communication plan.

Below are additional resources and steps you can take to strengthen the cybersecurity of your legislative office and legislature at large:

- Seek verification of your various social media platforms, including Facebook and Instagram (embedded links include verification guidance), to distinguish your official accounts from imposters.

- Use a Virtual Private Network (VPN): VPNs help protect against intruders when on public Wi-Fi; consider ExpressVPN or TunnelBear. Beware of free services, as they may steal your data.

- Use advanced threat-protection services to monitor malicious activity, such as CrowdStrike Falcon or Mandiant FireEye.

- Consider conducting a cybersecurity assessment with the Ford Foundation's Cybersecurity Assessment Tool to better understand the strengths and needs of your personal office and legislature.

- Use Security Planner to keep your data secure with a personalized plan, including customized recommendations to safely back up files, browse online without tracking, avoid phishing scams and prevent identity theft.

- To help think through how best to set up security policies, reference SOAP: Securing Organizations with Automated Policymaking.

For more thorough and advanced cyerbsecurity guidance, including the most up-to-date resources, please refer to the Design 4 Democracy Coalition's Resource page.

ENSURING THE CONTINUATION OF CORE FUNCTIONS

Legislation Development

One of the unique and critical roles of a legislature is to develop legislation; as a primary function, legislation development and all steps involved should be prioritized as functions are shifted online. Whether legislation is developed in response to a government proposal or a member's motion, legislation provides the authority by which governmental agencies function and influences the public policies governments adopt. In times of crisis, it is critical that legislatures can develop and pass laws that modify how they are able to conduct legislative business, direct governmental resources where they are most needed and support citizens' needs.

The legislation-development process is typically resource intensive and involves many hours of revisions and negotiations. During a crisis, however, the following standard processes may be truncated to expedite legislation development.

Examples of legislative processes that can be conducted remotely and digitally:

Authoring & Drafting Legislation

Introducing Legislation

Voting on Legislation

Authoring and Drafting Legislation

New or proposed legislation often amends already-enacted legislation or includes language from bills that were introduced but not adopted. Thus, it is imperative that staff has remote access to legislative resources. For example, staff in the U.S. Congress have access to secure online databases of enacted and introduced legislation that are only accessible while on site or remotely via VPN. While the Congress provides public-facing websites that allow citizens to access this information, the proprietary databases accessed via web interfaces from congressional offices provide more expansive search functionality that is helpful to those authoring legislation. It is critical that members and staff working remotely install the necessary VPN on their desktops and have the technical capacity, including adequate broadband, to access these resources.

Legislation development requires extensive coordination between authors and drafters. Authors, typically members and staff, will collaborate on multiple versions in an iterative process before legislative text is finalized. Once members and staff agree on final legislative text, legislative counsel drafts the final version of the bill. Authors and drafters can work and collaborate remotely if they have access to email, word-processing software and a document management system.

The legislative process can involve staff from a single member's office or from diverse member offices and political parties who must be able to share feedback on provisions in the legislation,

sometimes confidentially. When legislatures are able to operate normally, authors will meet in person or use the phone to have confidential conversations regarding legislative provisions that staff or members either want to change or remove from the legislation. Any process designed to transition legislation development online must account for the private negotiations that occur among members or staff. It is important to keep in mind that these negotiations are critical to the legislative-development process; negotiation often occurs both between legislators and among varying political factions within the parliament, and is key to the advancement of legislation. These negotiations traditionally take place in myriad ways, including during committee sessions, in legislators' offices, and even within the legislature's cafeterias and halls. To ensure negotiations are able to proceed, it is critical to ensure a sound digital-telecommunication sphere exists to allow members to converge and discuss.

Since authoring legislation is such a collaborative and sometimes confidential endeavor, members and staff working remotely must be able to share comments and edits to drafts in a timely and secure manner. For routine exchanges, encrypted email and secure file sharing typically suffice. Tools such as OnionShare allow secure and anonymous file sharing of any size without the involvement of any third parties, and can be used to share critical resources with individuals or groups. During any digital communications, it is critical to keep your VPN activated. For more informal or real-time conversations, authors may choose to use Signal or WhatsApp, both of which provide end-to-end encryption to secure conversations and documents on smartphones and desktops, ensuring only those granted access are able to participate.

Introducing Legislation

Following the completion of legislative drafting, the first step is for legislation to be introduced to the larger legislature. By way of example, in the U.S. Senate — a legislative body that continues to require members and staff to conduct most legislative business in person — members

introduce legislation by physically taking a hard copy of the legislation to the clerk in the cloak room of the U.S. Capitol. Each piece of legislation must include the introducing member's signature, as well as the signatures of any cosigners. Once it has been formally introduced, the bill is then assigned to a committee whose members will research, discuss and make changes to the bill — it is then put before that chamber to be voted on. Most legislatures follow some variant of this model.

For legislatures seeking to replicate this process online, there would need to be a digital means for collecting member signatures, as well as a secure online process for introducing legislation to the equivalent of the cloak room in the U.S. Senate. To do so, a virtual cloak room may be created with a secure email address that members may email with a copy of the legislation they'd like to introduce — this digital adaptation of the legislative-introduction process was successfully adopted by the U.S. House of Representatives.

Other legislatures that already use some form of digital voting are well poised to introduce legislation digitally, although this does not necessarily mean remotely. For example, the North Carolina state legislature amended its rules in response to COVID-19 to allow members to use their electronic dashboards to introduce legislation to the principal clerk's office rather than requiring the member to physically submit the legislation. The rule change allowed cosponsors to submit cosponsor requests via electronic dashboards to avoid the difficulty of capturing member signatures remotely. While this decreased physical contact between members and clerks, this did not make the introduction process a remote process; members must be physically present in the legislature to use their electronic dashboards.

An important piece of the legislative process is the incorporation of and opportunity for citizen feedback and engagement. As operations related to the legislative process are moved online, it is critical to find ways to continue to facilitate citizen feedback on draft legislation. Multiple tools can be used to allow for citizens and civil society groups to review, comment and provide feedback throughout the legislative process, including online portals, mobile apps and online surveys. For example, the Congress of Brazil makes use of an online portal, e-Democracia, to provide space for citizens to present legislative topics for online discussion or to comment on specific legislative proposals. Similarly, the Senate in Chile originally established Senador Virtual, now Congreso Virtual, an online portal allowing citizens to provide input on draft bills currently being debated in the Senate; citizens can vote on entire bills or on specific aspects of each bill, in addition to submitting comments. Even more direct engagement can be facilitated through the creation of platforms that allow citizens to directly submit legislative proposals for consideration by the parliament — online platforms for such direct participation have been created by legislatures in Canada, Panama and Costa Rica, to name a few.

For extensive guidance on how best to facilitate citizen participation in the legislative process and why it's important, reference this Citizen Participation Toolkit, created by ParlAmericas as a comprehensive guide for legislatures moving toward legislative openness.

Committee Meetings and Hearings

Committees play a vital role in the legislative process, including in the consideration of bills and issues during business meetings and exercising oversight over ongoing governmental operations in public hearings. As referenced above, legislative committees have jurisdiction over specific issue sets and governmental agencies, as well as the legislation that impacts them. As such, it is during a business meeting that committee leadership often decides which legislation introduced to the clerk's office will be considered by the full legislature on a specific issue. Committees additionally have the power to organize public hearings as a tool to hold executive-branch officials publicly accountable to citizens. While it is difficult to replicate these in-person meetings and hearings online, many

legislatures have taken steps to do this in response to COVID-19, allowing for hybrid proceedings that take place concurrently in person and online.

Business meetings and hearings are examples of key committee functions that can be performed online.

Business Meetings

Once committee leadership decides which of the introduced legislation to consider and send to the full legislature, leadership notices a business meeting during which committee members markup legislation by offering amendments before voting on the amended legislation. These meetings are usually not open to the public. Members, their senior staff and subject matter experts typically attend, along with committee clerks who record the meeting's proceedings and votes. Depending on the legislation being considered, contentious debate can occur among members. While it is difficult to replicate the human interactions that occur during these meetings, in times of crisis this process can be taken online via a secure virtual telecommunications platform for hosting online meetings.

In moving online, it is critical to consider that the clerk, who serves as the committee's record keeper and coordinates the administrative and IT functions for the committee, must be able to perform these broad functions remotely. In order to do so, clerks would need VPN access to the legislature's online resources, the ability to communicate with the clerks who manage legislative functions in the full legislature and the means to manage IT and administrative needs that may arise for members and staff working offsite. Clerks could use secure email and mobile phones to conduct much of this business. For sensitive or confidential exchanges, they may choose to use encrypted services such as WhatsApp or Signal. Platforms such as Riseup Pads or Google Docs may be used to create committee agendas and collaboratively take notes, if needed; while more secure platforms exist, these serve as accessible and free resources to consider.

▶ CASE STUDY: NEW ZEALAND

In response to the pandemic, voting was limited to committee meetings in the Parliament of New Zealand, where an individual is able to vote remotely via voice vote. The Parliament uses a video conferencing platform for remote meetings, in conjunction with in-house document-management software (SharePoint and Objective). This file-management system allows committees to view documents remotely, and for the documents to be held and managed on internal servers.

Remote committee meetings have been held in Ukraine through videoconference. All members are provided with a tablet with a pre-installed VPN for enhanced security. Members have access to the electronic document-management system and electronic-bill system, both of which have been developed on SharePoint Apps platform with add-ins: provider-hosted apps; and MS SharePoint Server 2016 Enterprise. Members also have access to electronic committee agendas, plenary agendas, email and citizen appeals made digitally via the same platform. MPs interact with this system by creating, registering and sharing e-documents, draft laws and amendments, in addition to tracking all phases of a committee legislative process by registering for a committee meeting.

If committees are unable to function fully remotely, committees may consider operating in a hybrid manner. The U.S. Senate and other legislatures, such as those in the U.K. and New Zealand, adopted rules to allow members joining remotely to vote via proxy. When voting by proxy, members who are present can cast votes for members who are absent or participating remotely. The speaker of the U.K. House of Commons outlined the process for members to request a certificate for voting by proxy, which includes emailing a specific email address in the parliament with the name of the member agreeing to act as proxy and a timeframe for the proxy to be active. The New Zealand Parliament determined that proxy votes can be used for the entirety of a party's membership in the House.

Hearings

Committees hold hearings to make executive-branch officials accountable to the public, to gather information about public policies and issues to inform legislation, and to make a political point. During times of crisis, it is critical that committees can convene hearings on the government's response to the crisis and hear the recommendations of elected and non-elected experts. Many legislatures have adjusted their rules to allow for entirely remote or hybrid hearings where some or all the participants testify via online-meeting platforms.

If committees choose to hold a hearing, staff should develop a communications plan for publicizing the hearing and its main findings widely. The following section (see page 32) on communicating with citizens during a crisis provides information on using social media, email and other mediums to reach constituents. As a strong example, the Federal Court of Australia, which shifted nearly all of its hearings online, developed a comprehensive tool to guide participants in accessing and attending virtual hearings and enable their easy participation.

Plenary Sessions and Voting

Plenary sessions have two main objectives: to allow for members to debate legislation and to vote on legislation. Elaborate rules, protocols and precedent govern these proceedings. When a crisis occurs, or when converting in-person operations to digital, it may be imperative to change or amend some of these rules to allow legislatures flexibility in how they operate, and some legislatures have done this to allow for digital, proxy or remote voting. However, fewer have changed the rules governing debate during plenary, and stil require members to be present to take the floor. Refer to page 8 for a list of examples of policies and procedures that have been adapted to facilitate remote operations.

Examples of plenary procedures that can be conducted remotely/digitally include debate and voting.

▶ CASE STUDY: INDIA

As a result of the COVID-19 pandemic, India has heavily instituted the use of virtual hearings, and has in fact favored the permanent integration of virtual hearings into India's legal system. After the onset of COVID, India's Supreme Court gave videoconferencing legal sanctity in the newly passed Article 142 of the constitution. While recognizing universal broadband and a lack of familiarity with ICT may pose a barrier, the Parliamentary Standing Committee on Personnel, Public Grievances, Law and Justice recommended that customized software and hardware be developed to facilitate virtual hearings to enable their continued use during COVID and beyond, with the hope that proceedings will become more streamlined and less expensive.

▶ CASE STUDY: ECUADOR

The National Assembly (NA) in Ecuador had its first virtual session on March 24, 2020, after a remote-session regulation was unanimously approved due to the COVID-19 pandemic. Since then, the NA commissions and plenary have been working remotely. The sessions are held through Zoom paired with the AnyDesk desktop application, but the voting system is still remotely connected to the voting center of each seat. The AnyDesk software connects with the NA's previously established voting system, known as Curul Electronica, which has been in operation since 2012, and is inclusive of functions such as biometric authentication, quorum verification, request to speak and electronic-voting mechanisms (previous manual available here). This remote work has facilitated the approval of some laws and resolutions to manage the health crisis and has created the possibility for assembly members to exercise oversight over the public policies arranged by the executive to manage the crisis. For an overview of the NA's system, review this short presentation.

To ensure the smooth operations of remote committee hearings, the National Assembly of Ecuador also took steps to invest in the training of support staff. In Ecuador, the parliament invested in trainings for the permanent secretaries of their respective committees on the various technical processes required to facilitate virtual hearings. Skills covered included operating video-conferencing systems; moderation of virtual sessions, including votes on proposals; and transmitting, processing and storing digital information. These trainings were conducted under the auspices of a new regulation that was passed to enable remote legislation operations (see page 8 for more details).

▶ CASE STUDY: ARMENIA
Successfully Transitioning Open and Closed Parliamentary Hearings Online

The National Assembly of Armenia, with the assistance of IRI, has been successful in shifting some of its parliamentary hearings online by piloting the use of Zoom and YouTube Live streaming services to hold parliamentary hearings — initially piloted with one public and one private hearing — for two standing committees. The Standing Committee on Science, Education, Culture, Diaspora, Youth and Sport (Standing Committee on Education) was the first committee to attempt to conduct an open virtual hearing, and successfully used Zoom to discuss online learning for schoolchildren as a result of COVID-19 school closures. Committee members, other MPs, the deputy minister of education, the head of the Government Agency for Educational Technologies, education experts, school principals, teachers and parents spoke about the challenges posed by teaching in this new format. The three-hour session was led by formal speeches and remarks, and concluded with a question-and-answer section where parents and teachers posed more than 50 questions to officials. To enhance the accessibility of the meeting, the hearing was livestreamed on the parliament's official YouTube channel, in addition to being livestreamed on the Facebook pages of participating officials. Multiple media outlets simultaneously livestreamed the hearing on their websites to maximize citizen outreach and parliamentary transparency. To view a checklist to guide the organization of online parliamentary oversight hearings, please view Apendix II.

The Standing Committee of Foreign Affairs used Zoom, YouTube and Facebook Live streaming to conduct a closed hearing to share and exchange important information regarding the COVID-19 crisis and ongoing response efforts. Seventeen registered panelists took part in the Zoom meeting; it was livestreamed by the parliament's YouTube channel, on Facebook by the Ministry of Foreign Affairs and several committee members, and by a very large number of media outlets, including on live television. These successes indicate the utility of piloting the use of virtual platforms to conduct and stream legislative activity in a transparent and accessible way. While these initial hearings were facilitated by the International Republican Institute, the National Assembly plans to utilize its own staff to run these virtual meetings moving forward.

Debate

Members debate issues and legislation during plenary sessions in a process critical to the functioning of a democracy. These sessions, which are available to the public, make the positions of members and the full legislature transparent to citizens and civil society organizations who seek to influence and hold legislators accountable. Especially during a crisis, citizens need to know that their elected representatives are working on their behalf. Thus, whether online or in person, it is necessary for legislatures to continue transparent debate during COVID-19.

While remote debate is technically possible, at the onset of COVID-19 many parliaments continued in-person debate. Respect for plenary and democratic traditions of transparency likely influenced this decision. In some regions, such as Europe, the relatively successful control of the

spread of COVID-19 may have also encouraged in-person meetings. Although legislators were required to physically take the floor to debate, legislatures adopted rules to protect members during plenary that required masks and/or social distancing while on the floor. Although the United States had one of the worst outbreaks of COVID-19, both houses of Congress required members to debate in person in their respective chambers. Both the House and the Senate implemented social distancing for members, and the House eventually mandated masks while in the House chamber. In Thailand, measures were introduced to facilitate continued in-person plenary sessions as necessary, while respecting public health concerns. Measures included required social distancing, working with a minimum number of MPs, redesigning seating arrangements for MPs during plenary sessions and the required use of face masks and temperature checks.[3]

Other countries have transitioned to online debate for plenary sessions. Although transitioning to online plenary debate is considered the safest way to ensure public health while continuing legislative operations, it can prove more challenging to achieve — both from a regulatory and technical standpoint — than the smaller task of shifting committee debate online. Some parliaments have leaned on existing digital tools to rapidly transition elements of plenary session online. For example, the U.K. Parliament made use of a preexisting tool created in 2017, MemberHub, to remotely submit questions by way of a parliamentary-specific VPN, using Microsoft logins as an authentication method. The below case studies provide examples of further approaches various parliaments have used to transfer plenary session debate online.

▶ CASE STUDY: CHILE

In Chile, recognizing that a majority of the parliament's members are part of the at-risk population for COVID-19, the Senate meets remotely via Zoom to debate issues ranging from extending postnatal leave to forbidding the denial of basic services during the epidemic. During deliberations, the chair of the committee is responsible for operating a clock that shows the timing of the session within Zoom, in addition to muting and unmuting members to maintain committee order. Each member appears on the screen and verbally states their vote. Legislation has already been passed using this method. For instance, legislation regulating access to unemployment insurance during exceptional circumstances was enacted in early April 2020 using this system (Source here).

---

[3] Actions and measures taken by the National Assembly of Thailand during the COVID-19 Pandemic. June 9, 2020. parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=69655&filename=index

The Parliament of Romania shifted to holding both plenary and committee meetings remotely in response to the pandemic. Standing orders of the Senate were adjusted to provide for remote operations in exceptional circumstances (such as epidemics, natural disasters, earthquakes or terrorist events). These remote plenary sittings are broadcast live on the Senate's webpage, with voting initially conducted over the phone by way of roll call, and then transitioning into the use of a new online tool to enable remote voting. This system requires the chairman of the plenary session to open the session and announce the start of the remote electronic voting procedure. From this moment, each parliamentarian has five minutes to select either "yes," "no," "ab" (abstention) and "no vote." At the end of the voting session, votes cast are displayed on the websites of the Chamber of Deputies and the Senate.

▶ **CASE STUDY: UKRAINE**

Prompted by the outbreak of COVID-19 and quarantine measures, the city of Dnipro became the first in Ukraine to hold a plenary session of its city council online. Although adjustments took place for city-level government, many of the same methods can be used to shift functions online for a national parliament as well. In order to make online sessions possible, the city council's Decision Implementation Office began preparation for the session 10 days in advance by drafting needed regulatory changes to be approved during the session, coordinating the training of local elected officials on how to use Zoom and facilitating several tests in small groups. The session started with a brief in-person meeting in the courtyard of the city council building, where council members maintained six feet of distance from one another. The council then voted to conduct further sessions online by adopting the drafted changes to the regulations of the city council and the rules on permanent commissions.

These changes legalized holding online sessions and meetings of city council commissions via the internet for the quarantine period. After a break, deputies resumed the session online using Zoom. During the online session, the council allocated 98 million hryvnia (UAH) for purchasing additional medical equipment, masks and gloves, and approved stricter measures on public traffic during the quarantine period. The city government is fully equipped with the technology and regulations needed to make the quick decisions that will be necessary in the future, and is well situated to provide oversight and communication regarding how public funds are being used to protect constituents' health and economic wellbeing.

Voting

It is critical that voting remain a secure process performed by the member. Legislatures have implemented various procedures to allow for members to vote on legislation during COVID-19, some allowing members to vote remotely and others requiring members to vote in person.

Proxy voting is one method that allowed for continued voting without the need for complex technical adjustments, but that still facilitated socital-distancing measures. For example, the U.S. Senate adjusted its rules to allow for voting by proxy in committee meetings; however, the full Senate still votes on legislation via an in-person roll-call vote with a verbal record of "yea" or "nay." No proxy voting is allowed on the Senate floor.

At the onset of COVID-19 the U.S. House of Representatives passed H.R. 965, which allowed for proxy voting on the floor of the House whereby members voting in person could vote for 10 additional members. Voting was also staggered for members so that no more than 50 representatives would be on the floor at one time. H.R. 965 also directed the Committee on House Administration to assess the feasibility of conducting remote voting should the need arise in the future. According to the committee's chairperson, in-person voting would be replaced with a secure email system and member-driven, remotely directed authorizations. The U.K. also amended its rules to allow for proxy voting in the House of Commons, as it did for voting in committee.

Due to travel restrictions throughout Europe, some members of the European Parliament were unable to vote in person. The European Parliament adjusted its voting procedures to allow for remote voting via email. Under this procedure, members received ballots via email, completed the ballot by hand, signed it, scanned or took a photo of it, and emailed the scan or photo to the central box in the European Parliament. This process was problematic for members who could not access printers and were unable to print their ballots. The European Parliament stated that it is

looking into procedures whereby remote voting could be entirely digital in the future. Implementing security protocols, such as two-factor authentication and digital signatures, could help to ensure the identity of members if the parliament transitions to email voting.

In the case of large pieces of legislation with numerous amendments, legislatures can vote on amendments one after another for many hours until voting on the underlying bill takes place. Typically, a chief of staff and/or legislative director will accompany their member to the floor of the legislature and coordinate remotely with senior staff on vote recommendations. They also monitor how other members vote before making recommendations to the member they advise. Depending on the legislation being considered, amendments may or may not be germane to the underlying bill, requiring input from staff that oversee diverse issue portfolios.

Some legislatures, such as the European Parliament, create an agenda so members can anticipate the votes they will cast. Others, such as the U.S. Senate, call up amendments at the will of the majority leader or the member managing a bill on the floor. In this case, staff typically receives the text of amendments beforehand via a secure internal website — accessed remotely via VPN — and send vote recommendations to senior staff via email for when the amendment is called for a vote. Staffers monitor floor proceedings and provide recommendations on amendments as they arise. If this process occurred online, staff would need a reliable platform to be able to monitor floor proceedings and access members' votes in real time, in order to provide accurate and timely information to the member they advise.

Finally, it is vital for the legislature's head or chief clerk to be able to perform his/her diverse functions remotely if digital voting is to occur. In the Minnesota House of Representatives, this includes maintaining records showing the status and progress of all bills, memorials and resolutions; ensuring the public is aware of and can access committee and subcommittee hearings; and

other administrative duties. In the U.K. House of Commons and other legislatures, the clerk of the full legislature sits on the floor of the legislature and acts as the adviser on all legislative procedure and business. The clerk frequently interfaces with members, their staffs and committee clerks. If a legislature moves debate and/or voting online, the clerk would need to have remote access at all times via a secure online-meeting-hosting service, VPN access to the legislature's records and resources, and a secure means of communicating with members or committee clerks who may have questions regarding procedure or other business, such as via WhatsApp or Signal.

▶ CASE STUDY: MALDIVES

As of March 30, 2020, the Maldivian parliament moved to fully use Microsoft Teams for virtual sessions, including committee meetings and plenaries. The parliament of the Maldives determined that remote meetings could be facilitated under its current rules of procedure, allowing virtual work to quickly begin without necessitating any amendments. In remote collaboration with parliamentary IT staff, legislators were assisted in setting up Microsoft Office 365 Business Premium on their respective devices. IT staff held many initial training sessions with members before Teams was fully implemented, and continues to provide ongoing technology training for members as needed to facilitate smooth use. All file sharing, debating and voting occur via Teams.

During sessions, only the speaker of parliament is physically present in the parliamentary chamber while all other members remain at home. One IT staff member is dedicated to facilitating plenary sessions, while two staff members are required to facilitate committee sessions. The livestreaming of all sessions is facilitated by one media staff member using social media platforms, primarily YouTube, with the same feed then distributed to all local television stations using a dedicated fiber network. Voting during sessions is conducted using a voting software add-on to Teams called Polly; if issues with Polly arise during a vote, members are asked to provide their vote by typing yes/no/abstain into the chat panel.

▶ CASE STUDY: BRAZIL

In Brazil, the National Congress adopted a new resolution to allow for both chambers to work remotely and to adopt virtual voting. The Chamber has instituted the use of Infoleg, an electronic voting platform available on both smartphones and tablets. The platform requires the use of a front-facing camera and two-step verification for debater authentication, records the full length of debates and allows the simultaneous access of up to 600 individual connections. In order to vote, lawmakers register their device in advance and sign in using a one-time password that is securely sent to their mobile device. Each

Brazil, cont.

session is limited to a single agenda item and a maximum duration of six hours, extendable only by the presidency for urgent matters. For detailed information on the platform, Sistema de Deliberacao Remota (SDR), used by the Brazilian Federal Senate to operate and vote remotely, including guidelines and templates for its use, visit this detailed website.

▶ CASE STUDY: BUREAU OF EUROPEAN PARLIAMENT

The Bureau of the European Parliament had agreed to temporary changes to the Rules of Procedure of the European Parliament to allow for remote participation and electronic voting by members in both plenary sessions and committee meetings. The new remote-participation procedure was first utilized on March 25 and remained in effect until July 31, 2020. During committee meetings, members were only able to remotely take the floor if authorized by the chair. However, during plenary sessions, only group leaders and specific representatives were allowed to intervene remotely. To vote, each member received a ballot via their official email address. The ballot, which was required to contain the name and vote of the member in a readable form in addition to the member's signature, had to be returned from their official email address to the committee or plenary services by the time the vote was closed in order to be counted.

▶ CASE STUDY: LATVIA

To safely continue operations during the pandemic, the Parliament of Latvia has employed a number of unique tactics to avoid in-person gatherings while continuing core legislative functions. In addition to holding some plenary sittings on eight separate parliamentary premises to ensure social-distancing requirements were met, the parliament also developed a new e-Saeima platform to allow plenary sittings to be held remotely while members debate and vote on items in the plenary agenda in real time. The platform is accessed using e-signature and requires a computer, Chrome web browser and internet connection. Upon activation of the voting mode, members have 30 seconds to vote either "for," "against" or "abstain." Remote plenary hearings using the e-Saeima platform are streamed live on the Parliament's Facebook account.

Executive Branch Oversight

Oversight is a critical component in a system of checks and balances, and is particularly important as all branches of government struggle to respond to the COVID-19 crisis. Conducting oversight — or the review, monitoring and supervision of the implementation of enacted legislation and public policy — is necessary to protect and enable strong democratic institutions and to strengthen a government's ability to serve and respond to citizens' needs. It is especially critical for a legislature to ensure that the executive branch is not taking advantage of the crisis to overstep the democratic boundaries of power.

Both members and their staff should feel empowered and responsible to conduct oversight over executive actions. While nothing replicates the legislative power of compelling government officials to respond to member and staff inquiries in person, the following procedures are available to legislatures when in-person exchanges are not possible.

Examples of oversight tools that can still be used remotely/digitally:

Online staff or member meetings.

Staff or member phone calls in lieu of meetings.

Member-led letters.

Cutting or increasing budgets.

Reports.

Question time.

Online staff or member meetings

Calling in administration officials to elaborate on policy in front of staff and members is a key element of legislative oversight of the executive branch. If this cannot be done in person, a secure online-meeting-hosting service could facilitate exchanges between the legislature and executive branch. A secure format for sharing documents before and after the meetings, in preparation for the discussion, would need to be established. Often, the executive will provide hard rather than soft copies of documents to disseminate at the meeting. One should assess whether the executive would be willing to send soft copies of these documents to the legislature before a meeting, and should carefully select the platform used to do so.

Staff or Member Phone Calls in Lieu of Meetings

If online meeting hosting services are unavailable, members and their staff could conduct meetings over the phone. While the phone does not replicate the face-to-face interactions of an online meeting, one-on-one and conference calls do provide an opportunity for the legislature to access and convey information to government officials. Consider providing access to long-distance calling for members and staff to facilitate communication across districts and constituencies, if required.

Member-Led Letters

Members send letters to senior administration officials to hold them accountable to the letter and intent of the laws passed by the legislature. They often include requests for information, express concern and urge action, or allow members to show publicly that they are actively performing oversight of the executive. Letters are especially powerful if followed by online meetings or phone calls with government officials who would be responsible for responding to issues or questions raised in the letter. These letters can be written individually; however, they are more powerful if legislators work together as a group to express an opinion or request. An example of a group letter written by the majority of the U.S. House of Representatives can be [reviewed here](#).

Cutting or Increasing Budgets

Legislatures hold the power of the purse. As such, it is imperative that legislatures continue to function during a crisis in order to direct resources to constituents, government agencies and services in response to where they are most needed. In order to maximize the financial impact, government agencies directing crisis response may see their budgets increase, while other agencies that do not have a role in crisis response may see their budgets decrease. An important additional power of the legislature is its authority to withhold budgets if governmental agencies are restricting democratic freedoms or are failing to fulfill their mandate as they respond to crises.

Appropriations committees have oversight over the budgets of governmental agencies. They pass legislation out of committee, including any budgetary increases or decreases, and send it to the full legislature for a vote. During a crisis, the leadership of the legislature may choose to bypass the formal process and send legislation directly to the floor for a vote. In the U.S. Senate, [Rule XIV](#) allows the majority leader to bypass committee and put a piece of legislation directly on the calendar for consideration by the full Senate. Rule XIV is a standing Senate rule that is available to members and the majority leader alike, so invoking it does not require a rule change. Legislatures without this rule may need to adopt it when a crisis arises to expedite the legislative process.

Reports

Legislatures can produce publicly available reports that assess the executive's crisis response. Members or committees can draft reports on individual policies or the executive's comprehensive policy response using information obtained during meetings with administration officials, memos prepared by the legislature's research service, research by academic institutions, news from respectable media outlets and research prepared by staff members who typically draft the reports. Depending on the topic, foreign embassies and officials have also helped to provide information for legislative reports, such as for the U.S. Senate Foreign Relations Committee's 2018 report entitled ["Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security."](#) European embassies provided open-source information to committee staff that aided in the report's preparation. During a global crisis like COVID-19, legislatures could work with their foreign counterparts to investigate and develop best practices in public-policy responses. It would be beneficial to develop a communications plan for publicizing a summary to ensure constituents have access to the report's findings.

Question Time

Some legislatures, such as the Estonian Riigikogu, allow for question time in each plenary, during which the prime minister and other ministers reply to questions from members of parliament. These opportunities are used to secure needed information, require transparency and enforce accountability on the part of the executive. Legislatures can attempt to replicate these sessions remotely via a secure online-meeting application.

Facilitating Internal Communication within the Legislature

While more formal communications such as party caucus meetings, public hearings and plenary sessions can directly translate to the virtual office suites described on page 11, and should be prioritized by the legislature as it moves online, it is important to maintain methods for informal communication between members and their staff.

Without thought and preparation, informal "pop-in" and water-cooler conversations can be some of the biggest losses for a parliamentary office when transitioning to a digital format. Informal communication is key to collaboration, information sharing and relationship building. By recognizing the value of informal interactions, parliaments can set up guidelines and structures that replicate functionality online without compromising on security or public access to information.

KEY POINTS FOR SECURE INTERNAL COMMUNICATION

- Security: Ensure all offices and staff are aware of the security features and vulnerabilities afforded by commonly used platforms (e.g., WhatsApp, SMS or Facebook Messenger). For maximum security, most experts recommend the encrypted messaging app Signal.

- Ensure all offices and staff understand how electronic information flows relate to rules and procedures that govern legislative business, especially with regard to freedom-of-information requests, interactions with the media and issues of the public record.

- Establish an office-specific code of conduct and, if possible, a legislature-wide code that applies to both formal and informal communications channels. Codes of conduct help to establish an inclusive, participatory culture. Expectations of what constitutes negative behavior and the penalties for engaging in such behavior should be made clear. Codes of conduct can include a wide range of rules depending on the desired outcome, but generally include prohibitions on, for instance, sexual harassment, discrimination and hate speech.

- Consider how best to promote "low stakes," unprompted interactions; think about what is gained from those interactions and how they may be recreated virtually. How can you best ensure serendipitous interactions are still happening?

- Issue-caucus meetings are a key way for members to informally organize and meet to discuss issues of mutual concern and possibly perform legislative research and policy planning. Create channels for members of issue caucuses to meet, organize and continue to informally discuss issues of shared interest.

- Consider utilizing tools that facilitate group communication and awareness, such as email lists, WhatsApp groups and Twitter lists.

Communications by and among legislative staff are also critical to the healthy functioning of a legislature and should be prioritized by each member office. Consider the following points to create a coordinated, inclusive and streamlined system for staff communications.

- The internal operations of a parliamentary office benefit from the use of both long-form and short-form communication platforms. Email often remains the preferred method for formal communication. It also often remains the preferred method of communication with external entities such as constituents and the media. However, shorter-form communications can be vital for the smooth operation of the office. Consider the following for shorter-form communications:

  - As staff members reach out to other offices and committees for coordination, encrypted informal communication pathways such as Signal can be vital for private deliberations that would otherwise have occurred in person.

  - Choose communications platforms that allow for the easy segmentation of conversations along topical lines to ensure that chats can be cleanly issue focused without cluttering out other vital messaging.

  - Internal office channels should be created to give staff members the option to discuss issue matters privately and candidly with their colleagues and to be confident in the privacy of these discussions.

  - Many platforms, including GChat, Slack and Teams, have "online" lights that mark one's availability. Actively using these lights can lead to more common spontaneous interactions within an office as quick returns can be expected.

- For committee offices that work with multiple individual members of parliament and their respective offices, clear informal and formal lines of communication (and which platforms are used for what purposes) will be especially important.

- Because committee staffs are typically smaller than the sum total of their members' offices, it is expected that a much higher proportion of committees' messaging will be formal communication between offices in order to coordinate between committee members in a transparent and accountable manner.

The above points illustrate the many concerns that should be considered by staff and members alike as internal legislative operations shift online. Clear and consistent internal communications, file storage and organizational structure are paramount to the successful functioning of a legislature.

COMMUNICATING AND WORKING WITH CONSTITUENTS

How effectively elected officials are able to externally communicate during a crisis can be the difference between a successful response that saves lives and staves off panic and a failed response that leaves citizens without guidance and an exacerbated public health crisis. The following section will focus on key aspects of external communication during a crisis: inclusive digital outreach, digital crisis communications, public health communications and available resources for your legislature to employ. Note that many of the tools and best practices provided below are applicable to non-crisis communications with constituents, offering a more cost-effective and efficient way to conduct outreach in normal operating circumstances.

When considering the implementation of any of the below tools, be sure to account for the increased support that will be required from legislative and IT staff. As the use of digital communications grows, you may need to expand communications and IT teams to ensure legislators are supported in the use of these new tools.

Messaging During a Crisis

Constituents look to public leaders to be a calm, clear source of stability and information in an otherwise unpredictable time. It is critical to invest in building trust and confidence with constituents at any point in office as a legislator or staffer, but this is even more critical during a crisis. If your citizens don't trust the institutions of government or the officials therein, they will be far less likely to listen to your guidance and direction (refer to An Open Government Approach to Rebuilding Citizen Trust for additional guidance on this topic). Throughout your time in office, and especially during a crisis, be sure to reach out, listen to citizens

and meaningfully respond to their needs. And as you communicate during a crisis, keep the following seven elements of effective crisis messaging in mind to serve as a clear and consistent leader.

1. **Express empathy:** Empathy lets people know you appreciate what is important and that you connect with and care about your constituents. Saying you are participating in the action with empathy lets constituents know you are leading with them in mind.

2. **Demonstrate vigilance:** This shows your audience that you are there, and that you are carefully and persistently working to address the crisis.

3. **Detail action being taken:** Detailing the action you are taking provides transparency. It is important to note that, when detailing action, you must stick with the facts! In part, your efforts are to give people information that will help them; panic and speculation rather than facts do not help anyone. Sharing the facts, even when they are grim, helps people to better understand the scope of the problem.

4. **Provide credible sources of information:** This helps prepare citizens to be successful survivors by empowering them to know where to find reliable information they need.

5. **Provide a call to action:** By giving your audience a job, you are helping its members to be part of the solution and to feel some sense of control. Even a task as simple as "wash your hands" or "check on your neighbors" can serve as an outlet for citizens who wish to take action.

6. **Follow-up and next steps:** Tell audience members how they can reach you. Be transparent about your next steps, what you plan to focus on and how you aim to do so. This sets clear expectations and can provide a sense of forward movement, even if it is in small, incremental steps.

7. **Recurring communication:** Finally, tell your audience when you will speak to them again, and clarify through what method and how frequently. Will it be an email or a press conference? Daily or weekly? Providing these details will create predictability in a situation that is otherwise uncertain.

Most importantly, never speculate. Remember that it is OK — and often necessary — to say, "I don't know." Although difficult, your recognition of unknowns provides an opportunity to be transparent with your audience, and to reassure them that you will take action to try to find an answer.

Public Health Communications

A critical component of communications during a public health crisis is ensuring you are communicating relevant, verified information to your constituents. Retweeting or reposting trusted, verified sources can be a helpful and time-efficient way to amplify important public health messages that will keep your constituents safe. As a public official, it is your job to provide your constituents with trusted facts — not rumors and unverified theories — to keep them safe and healthy, and to stave off panic created by misinformation.

False information about the COVID-19 pandemic is rampant — future crises will face the same deluge of misinformation and disinformation. The rapidly changing situation creates desperation for information, leaving people vulnerable to misinformation. As an elected official, you should actively counter false news with reliable information of your own. Proactively and consistently confront rumors and conspiracy theories with the fact-based truth, supported by multiple reliable, non-partisan sources. A few

international sources you can look to for fact-based recommendations include, but are not limited to:

- The World Health Organization.
- Centers for Disease Control and Prevention.
- The National Health Service.

As you seek reliable news to relay to your citizens, it is important that you actively avoid misinformation, and inform citizens as to how they can best avoid misinformation related to the pandemic as well. Turn to domestic sources that rely on thorough, nonpolitical research to communicate truths to constituents. This article, How to Avoid Misinformation About COVID-19, provides a starting point to help you learn how to identify and avoid false information.

Access and Inclusion Online

Don't forget to think critically about the platform you will use to communicate these messages, with a keen eye toward inclusivity. Online programming can exclude the participation of significant and often vulnerable demographics. Consider how to include vulnerable demographics in your digital crisis-communication plan by choosing platforms that are free or widely accessible, communicating at times of the day that allow women or youth to join and directly reaching out to those who may need more targeted contact, such as the elderly. Given the breadth of socioeconomic variables that affect digital access and inclusion, there is no one-size-fits-all digital outreach strategy. Diversifying your communication-platform use will help you reach larger portions of the population and will ensure you are reaching your audience in a democratic and inclusive way. Mass robocalls can be used to reach those without internet; call-in hotlines using an interactive voice-response system can share prerecorded information and facilitate routing callers to the most appropriate assistance; WhatsApp messages can target cellphone users and live press conferences reach those with access to streaming services.

Who has access to the internet? Who doesn't?

The "who" should take into account economic inequality, urban versus rural, ethnicity, religion, tribal internet access and habits, gender, age and any other notable indicators that impact internet access in the community you are trying to reach. If there are groups that have no access, consider augmenting digital outreach with targeted communications to those groups using accessible tools such as phone calls and short message service (SMS) messages, and — if appropriate for your context — including a call to action for word-of-mouth campaigns in digital communications.

How fast is the internet access of those you want to reach? Are there inequities in internet speeds?

In general, live video with multiple participants requires high-speed internet; live video from a single person requires moderately high-speed internet. Recorded videos can be more easily played back in low-speed environments, but still require a reasonable internet connection. Small infographics and pictures will work for most and text posts require limited connections. Direct messages over platforms such as WhatsApp, Telegram or Signal require very little bandwidth. If you are trying to reach low-income groups in rural areas whose internet speeds are slow, a live video conference will be ineffective.

How do your constituents access the internet?

People access the internet in various ways: smartphones, internet cafes, libraries, a shared home computer and/or personal computers. Do different groups within your constituency access the internet in different ways?

As a general rule, **make sure your content is smartphone friendly** as this is how most people consume content online. Most major platforms today are built for mobile access, but government websites often are not. This is easy to fix; if you post a video or piece of information on your official website, be sure to also post it across other platforms. To reach those with older phones, be sure to communicate critical information through simple SMS messages as well.

Also consider **privacy and safety.** If the information you are sharing is sensitive, or if it would indicate something personal about the person reading it (e.g., an announcement about sexually transmitted disease testing to at-risk communities), consider the implications of that information being consumed on a shared device or in a public setting.

Finally, consider **cost barriers** for your constituents. While an individual or household may have access to the internet, the cost of data or other costs associated with connecting to the internet may prohibit some from engaging. Consider supplementing live streaming of events with messages broadcast on the radio or TV to reach those facing cost barriers to internet use.

What social media platforms and information sources do your constituents already use?

Different demographic groups use different social media platforms. This is not consistent across contexts; as such, there is no one-size-fits-all approach. However, in general, Twitter is often used by elites and journalists, making it an excellent communication mechanism if you are looking to have your message amplified by the press. Facebook is popular across demographic groups, and some carriers allow access without incurring any data charges. TikTok and Instagram tend to be used by younger demographics. Content style and distribution should be tailored to the audience you are trying to reach (see page 36 for guidance on use of social media platforms).

For those who are unlikely to receive your message directly through online messaging, consider the following:

- Include a request for word-of-mouth sharing in your digital communications. For example, if only young people are likely to see your Instagram post but they live in an intergenerational household, a call to action that encourages them to share the information with their families may be effective.

- Target outreach to specific communities/demographics. This should be responsive to the communications habits and trust structures of your target audience. If you have been able to reach the vast majority of your constituency online, but have not been able to reach the elderly, consider what communications channels they use and create a campaign specifically for them. You may augment your digital outreach with radio interviews/announcements, sending physical letters or working with other community leaders who are accustomed to communicating with those groups.

- Not all constituents have access to, or are proficient in, technology used for digital communications; thus, legislatures may need to supplement the technological solutions and strategies presented above with ones that are more analog. For example, some constituents only contact

their representatives via cellphones (not smartphones) or landlines. To ensure all citizens are able to reach their representatives during crises, legislatures could consider implementing a central phone bank with one assigned phone number that could be routed to a member's designated staff. The designated staff could be on call during regular business hours or designate specific times that he/she would be available to receive calls. If constituents called outside of normal business hours or were unable to reach staff, they could leave a message that staff could return in a timely manner. Members could also pre-record important information that constituents would hear before connecting with a staff member. This would increase accessibility for constituents who rely on phone calls, rather than emails, text messages or the internet to communicate with and seek answers from their representatives.

Using digital communication to increase accessibility:

Digital communication allows for the rapid creation and distribution of content in multiple different formats, which can help elected officials reach more people, including those who have historically been left out. Make sure your content can be consumed in a number of different ways. For instance, if you create a video message or are conducting a videoconference, turn on automatic subtitles or use a platform that includes that feature as an option to ensure that those who are hard of hearing or who otherwise cannot listen to sound (shared household, sensitive content, etc.) can read the text. If you create a text-based piece of content, ensure it is machine readable so that those who are blind or illiterate can listen.

The 18f Accessibility Guide includes in-depth tips and resources for ensuring online engagement is as inclusive as possible.

Communication Tools and Platforms
Mass Communication: How and Why to Use It

Reaching as many constituents as possible with urgent, timely and relevant information is key during any crisis. Mass-communication tools can most easily and effectively reach large portions of your constituency and can help ameliorate communication problems your legislature may face, especially in reaching rural or isolated communities, and are especially important to share public-service announcements or important alerts. Two of the most effective and accessible forms of mass communication are SMS and email. With either method, it is important to identify the goals and objectives of your message in advance to make it easier to shape messaging content.

In order to communicate successfully via email or SMS, you will have to collect contact information — the email addresses and/or phone numbers — of your constituents. Adding a subscription field to the homepage of your legislature's website, asking constituents for email addresses during phone conversations or collecting contact information via special-event registrations are good ways to collect the needed information.

SMS MESSAGES can reach anyone who has a cellphone. These messages provide the opportunity for officials to send short updates about important or urgent information related to the crisis, and can be sent in bulk. While SMS messages should be limited in use for short communications of time-sensitive information, they provide the opportunity for real-time constituent communications as well as two-way communications. Be sure to use clear, concise messaging to avoid constituents confusing your messaging as spam.

EMAIL messages are best used to send longer, less time-sensitive updates and more detailed information to constituents. Email messages can be used to drive constituents to specific resources by linking relevant websites or information internally in the email. A key benefit of email is that it enables the sending of customized messages at very little cost. Examples of uses for email campaigns include informing constituents of upcoming events, building awareness of an issue, informing volunteers of the latest news or driving constituents to complete an online survey. A listserv can be used to store and maintain constituents' email addresses, and enables the easy dissemination of mass communications. Keep in mind that some constituents create an email account simply as a method to join other social media platforms; to reach the broadest segment of your constituency, remember to use multiple tools to share the same message.

There is extensive guidance available online on best practices for the use of the above tools. For accessibility, we have summarized the basics of the available features and some best practices for each platform below:

FACEBOOK FOR GOVERNMENT, POLITICS AND ADVOCACY:

The basics: As a public leader, it is critical to have separate personal and official Facebook accounts. This is necessary because it provides an extra layer of security, in addition to allowing you to interact differently with constituents than you would with family and friends. Enabling two-factor authentication, a security mechanism that requires you to enter a specific code when someone tries to access your account from an unrecognized account, is a simple step to protect your information and presence on Facebook.

For people and organizations involved in politics, it is recommended to use a Facebook Page. A Page is a public presence designed for connecting at scale with people who you may or may not know personally. In order to better reach and connect with your audience, Pages provide access to tools such as insights to track engagement metrics, civic-engagement tools, mobile apps and the option to advertise.

- If you are a government official, select Community or Public Figure, and then select the Government Official option.

- If you are a government organization (such as police or fire department, city council or other government department or agency), select Community or Public Figure, and then select Government Organization.

- If you're setting up a page for a political organization (such as a political party or other political advocacy group), select Community or Public Figure, and then select Political Organization.

For step-by-step guidance on how to get the most of your Facebook presence as a public official, refer to Facebook's Learn the Basics Guide written specifically for users in the government, politics and advocacy spaces to outline best practices and latest tools.

▶ **CASE STUDY: NAMIBIA**
BeLive Facebook Streaming

Prompted by the COVID-19 crisis, the National Assembly of Namibia has been meeting virtually for the first time in its history. To meet procedural requirements, 50 members were physically present in the plenary chamber to ensure a quorum of voting members, while the remaining members connected via online video link to separate meeting rooms. The National Assembly's live streaming services were expanded to multiple online spaces, including the parliament's website, with translation into indigenous languages. The audio files could then be used by radio stations to broadcast to the electorate, in keeping with the parliament's commitment to reach the grassroots. The parliament's Facebook page now reaches more than 70,000 users daily (increased from 1,000 before the lockdown) partly due to the live streaming. For additional guidance on using Facebook Live in your own legislature, refer to Facebook's Tips for Using Facebook Live guide.

INSTAGRAM FOR POLITICS AND GOVERNMENT

The basics: Instagram offers a more visually compelling way to engage your constituents and reach large, new audiences through photos, videos, stories and messages. It is recommended that politicians and public figures use the "Creator" account type, which offers a unique profile appearance and more advanced user insights to better track constituent engagement. Instagram offers a variety of different avenues to share your content and messaging, including:

- **Feed:** This is the place to post content you want to remain visible on your profile and be visible to people scrolling through their timelines.

- **Stories:** Stories posts remain visible for 24 hours. They can be used to broadcast live Q&A sessions or interviews, and to invite constituents to participate and ask questions.

- **Direct messaging:** Functioning as a private messaging inbox, this is where you can receive one-on-one messages from your constituents or followers.

- **IGTV:** Used for posting long-form videos, up to 60 minutes long. This is an ideal place to post full-length speeches or panel appearances.

- **Reels:** Used to record and edit 15-second multi-clip videos with audio, effects and creative tools. These can be shared with your followers on your Feed, or can be made available to the wider Instagram community through the Explore feature.

Instagram Insights can be used to track engagement and day-by-day progress, including a detailed overview of how and why your account grows (or does not grow) each day in a given week, and how many follows and unfollows your account receives. For a detailed guide on how to use each of these features, including recommendations for best practices, please reference this guide.

TWITTER FOR GOVERNMENT

The basics: Twitter facilitates short, rapid interactions that allow public servants and their constituents to regain direct contact, and offers new techniques for listening to, mobilizing and informing your constituents. Twitter messages were designed primarily for use on a mobile phone, with tweets limited to 140 characters to mimic the length of a text message. Twitter is a useful medium for sharing the latest crisis information, providing rapid updates, promoting your efforts as a public official and announcing available services and events. A tweet can be used for messages that are 140 characters in length or to share a link, photo, video or a combination of all four. Some of the key available features on Twitter include:

- ■ **Direct message:** Allows you to start a private conversation or create a group conversation with anyone who follows you.

- ■ **Twitter Live:** Share your stories as they unfold with live video; you can broadcast live from events or share a scene of a breaking news event to better inform and connect with your constituents.

- ■ **Lists:** Twitter lists can be used to organize and read tweets from a select group, allowing you to keep track of what groups of key opinion formers are saying, including your political colleagues or constituents.

Tweeting behind-the-scenes content, including a call to action and using hashtags boosts viewership and allows you to more closely and frequently connect with constituents. For the most updated step-by-step guidance on how to set up a Twitter account and follow best practices, please view The Twitter Government and Elections Handbook or the handbook for NGOs, Politics and Public Service.

WHATSAPP FOR GOVERNMENTS

The basics: The ease of use and wide accessibility of WhatsApp has made it an extremely popular global platform, with 1.5 billion users worldwide. WhatsApp provides messaging, internet voice and video calling, document sharing and more on both your mobile phone and desktop with complete end-to-end encryption. It is recommended that public officials use the WhatsApp Business app to best manage multiple questions and feature helpful information for your constituents; it is free to download. Services available on the business app include:

- ■ The ability to create a short link that community members can use to initiate a private WhatsApp chat. This link can be shared through email, your website or Facebook Page.

- ■ Build your profile to set up custom greeting messages so people know where to find resources and more information about available services.

- ■ Use the catalog to showcase and describe services available to your constituents.

- ■ Use photos, video and text to feature accurate and timely information in a status update.

For the most up-to-date guidance and additional information, visit WhatsApp's page with recommendations for using the WhatsApp business app to Stay Connected During the COVID-19 Pandemic.

Timor-Leste launched a dedicated service on WhatsApp to provide information to citizens during the COVID-19 pandemic. The service, available in both Tetun and English, is being provided on a new WhatsApp information channel as part of the multipronged preparedness and response by the Ministry of Health to provide timely information, contain rumors and counter misinformation. For those without mobile phones connected to the internet, the Ministry of Health has been sharing information via SMS.

TELEGRAM

The basics: Telegram is a messaging app with a focus on speed, security and accessibility, with end-to-end encrypted voice calls. Telegram can be used on phones, tablets or computers and can allow you to create group messages for up to 200,000 people, in addition to using channels for broadcasting to unlimited audiences. While not as widely used as WhatsApp, Telegram offers many similarly useful features. Available services include:

■ **Telegram Channels:** Channels can be used to broadcast important information to a very large audience; they can be public or private. If public, they can be searched for and found by anyone, and offer a great way to share public health updates. Only one-way communication is possible.

■ **Groups:** Group messages are ideal for collaboration in smaller, more targeted teams, although they can grow to communities of up to 200,000 members. Groups allow for two-way communication.

For the most up-to-date information on Telegram and its available features, please visit Telegram's webpage.

SIGNAL

The basics: Signal is an easy-to-use, free, end-to-end encrypted messaging platform that additionally offers voice and video call features. Signal is free to use and functions across mobile and desktop platforms (on Android, iOS and Chrome) with features including group messaging, private messaging and extremely high privacy standards. Signal is recommended for sensitive communications between individuals and groups. For the most up-to-date information about Signal, please visit Signal's webpage.

YOUTUBE

The basics: YouTube offers an accessible platform to engage with citizens on what's currently happening in your legislature through video. YouTube offers you the ability to create your own channel where you can upload videos, curate your own content and even livestream public hearings and committee sessions. With more than one billion active users, YouTube serves as the internet's second-largest search engine and is an important platform to use to reach your constituents. Available services include:

- **Brand account:** A brand account allows users to manage editing permissions, grant access to the account for multiple team members and create a more holistic online presence. Create multiple content-specific channels within your brand account for greater focus and ease of use.

- **YouTube Live:** This feature allows users to broadcast live content to viewers and can allow your audience to participate with real-time comments, questions and reactions. You can livestream using a webcam, mobile cam or encoder streaming.

For the most updated guidance on creating and using a YouTube account to connect with citizens, please visit the YouTube Creators website for how-to videos and key tips and tools.

JITSI MEET

The basics: An alternative voice and video conference platform, Jitsi Meet is a secure and free option for voice and video meetings. It is encrypted, open source and does not require accounts to use it; this may make the platform easier and safer to use than similar counterparts. Jitsi Meet is functional on both mobile and desktops, and can be used through Slack as well. Features include text chatting, screen sharing, streaming to YouTube Live and other features similar to Zoom or Skype video conferencing platforms.

VIDEOCONFERENCE TOWNHALL: BEST PRACTICES

For legislatures interested in employing one or multiple of the above tools to hold a videoconference townhall, please consider the best practices listed below:

- Make recordings and transcripts available for those with low internet bandwidth or who are otherwise unable to attend in real time.

- Set rules for the townhall ahead of time, and lay them out clearly at the beginning of the townhall. What will the structure of the townhall be? How should people signal that they would like to ask a question or make a comment? What are the time limits on talking? Will there be a chat function and will staff be engaged in the chat function? Should people have video on or off?

- Video conferences require logistical preparation and a gameday plan, with clearly assigned roles for staff. Those might include:

  - Providing technical support to participants.

  - Monitoring the chat, raised hands or answering questions/comments.

  - Providing reference documents/links relevant to issues that come up during the townhall.

  - Muting and unmuting people, admitting people into the videoconference if you have a lobby feature turned on, verifying identities.

- There are a number of platforms available. You should take into account which platform your audience is already most likely to be using, what tools are needed (e.g., lobby, chat, raise hand, multiple videos), and what your security requirements are.

MAILCHIMP

The basics: Mailchimp can be a useful tool for generating email campaigns to conduct outreach and information campaigns. Mailchimp offers easy-to-use guides to generate email templates and lists to send important information in an easily digestible and clear way. Available services include setting certain emails on autopilot to reduce some of the emailing workload, such as setting welcome emails to automatically send to new subscribers, in addition to audience segmentation to facilitate the creation of targeted message campaigns.

VIAMO

The basics: If a lack of connectivity and tech infrastructure poses a limitation to communicating with your constituency, Viamo focuses on supporting communications via the much more widely accessible platform of mobile phones. Viamo offers SMS and interactive voice response-based systems for reaching citizens on mobile, and has launched specific COVID-19 resources to increase community awareness of and ability to communicate regarding COVID-19 updates. Viamo has partnered with governments and civil society to strengthen health messaging systems; for more information, visit Viamo's webpage.

TELERIVET

The basics: Similarly to Viamo, Telerivet is a mobile messaging platform that can facilitate connections with your constituency if low technical capacity — on the part of the legislature or of constituents — poses a barrier. Use of the platform requires only a standard mobile phone and does not necessitate servers, programmers or contracts. A cloud-based management system routes messages to anyone with a mobile phone with SMS, and can easily be used even in remote areas. For more information about available services, visit Telerivet's webpage.

BLOGS

The basics: Blogs are a useful platform for longer-form communications with constituents. They can be used to informally share ideas and updates, and provide an opportunity to expand upon press releases and in-depth guidance that is otherwise limited by message-length restrictions on other social media platforms. There are many free and easy to use platforms for blogs, including WordPress and Blogger. Blogs can easily be linked and shared within emails to constituents, which may expand your constituent reach to those who may not be familiar or comfortable with social media platforms.

KEY RECOMMENDATION: DEVELOP A SOCIAL MEDIA STRATEGY!

Regardless of the tool — or tools — you choose to use to engage with constituents, it is important to develop a strong social media and content strategy to organize and manage your communication and distribution of information across multiple platforms. You should aim to integrate this social media strategy into the larger communications plan of your office. As you select your preferred communication tools, consider simultaneously planning for the following:

- **Develop a content strategy for your social media platforms** to be sure you are best amplifying and coordinating your online activity. This means planning ahead on some of the general content you would like to post, such as preparing preplanned event announcements, public-service announcements and preselected video and photo media. Remain cognizant of the information you and your legislature would like to most heavily promote, and center your strategy around those key messages.

- **Using a social media calendar** is a great way to remain strategically organized days, or even weeks, in advance. Having a clear social media calendar will also help to visualize and maintain the regularity with which you'd like to post. Use it to list the dates and times you'd like to publish different types of content on each channel. A simple handwritten calendar, a spreadsheet or more advanced software services can be used to organize and schedule social posts in advance, and can detail the specific content, the platform to be used and the timeline on which it should be released.

- **Use consistent branding,** such as standardizing logos and images, across networks so that your social media accounts are easily recognizable and verifiable.

Organizing and Engaging Citizens

Citizen engagement, one of the most important responsibilities of a legislator, is made ever more important by the onset of the COVID-19 crisis. Citizens are relying on you to be a voice of reason, reassurance and truth — and to help direct their response efforts. There are multiple tools that can be used to continue to engage with and empower your citizens to create meaningful interactions digitally.

While traditional methods of citizen engagement might rely on visiting constituents in their local communities, whether that be in their homes, local schools or religious spaces, the spread of COVID-19 necessitates innovation toward digital engagement. The following section outlines some of the options that can be used to facilitate citizen mobilization and engagement while still following public-safety protocols. Combining a variety of these engagement methods will help you to reach a broader and more diverse constituency, ensuring important updates and public-service announcements are heard by as many constituency groups as possible.

METHODS OF ENGAGEMENT AVAILABLE IN CRISES AND BEYOND:

WRITTEN MATERIALS: constituent correspondence letters; postcard mailings, opinion-editorials, letters to the editor, newsletters (Mailchimp), etc. These written materials can be written and promoted by staff or members. Also consider communicating with constituents through newspapers and bulletins in public spaces.

VERBAL COMMUNICATIONS: direct phone calls.

BROADCAST: TV, radio and podcast interviews.

DIGITAL QUESTION-AND-ANSWER SESSIONS with constituencies via videoconferencing.
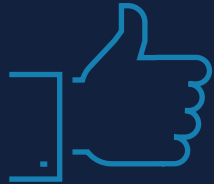
CALL-IN "OFFICE HOURS" for constituents who may not have internet access.

Access to parliamentarians and staff via a **SECURE MESSENGER**, such as WhatsApp or Signal.

VISUALS: If literacy is low among your constituency, consider using graphics, cartoons and/or visually geared posters in public places to share important information that is easy to comprehend.

SOCIAL MEDIA: Facebook Live, tele-townhall, tweeting and Instagramming daily operations (see page 37 for more detailed guidance on available social media platforms).

AN ONLINE INFO-BULLETIN to constituents to inform them of official sources of information regarding the situation and resources available to them, updated in a consistent and timely way.

UPDATES TO GUIDELINES on how to communicate with the parliamentary departments and government agencies responsible for access to information, citizen participation and public health.

POST FREQUENT REMINDERS of where the public can find live transmission of plenary sittings online, on the parliamentary television network or on the radio.

CONDUCT VIRTUAL OUTREACH TO COMMUNITY ORGANIZATIONS — such as health centers, food banks, women's shelters, etc. — to identify required support.

These suggestions for methods to engage with your constituency are just the tip of the iceberg; there are many more ways to engage with citizens and the organizations that serve them even if you cannot visit in-person. For additional best practices on how to use social media to engage with constituents, visit the Digital Tools and Content chapter of IRI's Serving as a Representative of the People: A Guide to Engaging Your Constituents. When possible, use legislative staff to support these initiatives, and brainstorm new ways to engage with a strong eye for inclusion. If your legislature is seeking a more in-depth guide to additional tools that might be used to engage citizens, visit ParlAmerica's website, ParlTools, to access a toolkit that walks legislatures through citizen participation in the legislative process.

How to Capitalize on and Build Online Communities

To take citizen engagement a step further, building online communities with and for your constituents is an effective way to disseminate important information and to mobilize citizens to plan, engage and assist each other and the government in its response measures. In a time of crisis, strong enablers of communication such as an online community and resulting coordinated citizen-response efforts can make a government response increasingly effective.

Have a clear sense of purpose. Everyone should know why they're there and what is expected of them.

Maintaining online networks requires active and consistent management. This should be reflected in your staffing plan.

Before you begin to build an online community, it is important to have a clear purpose and develop a maintenance plan.

To create the most useful online community, take the time to first consider the purpose of the group, which will then clarify who are the right people to include. Will this group serve to share information on a specific issue area? Will the group foster mutual support among your constituents in this time of crisis? Based on the intent, you can then intentionally add the right people to foster the intended dialogue and group culture.

Information sharing on an issue or area

Fostering collaboration to advance a specific project or goal

Mutual support

Coordination

Facilitating member-driven programming

1. Start small. Really small. People should feel awkward if they aren't participating. It helps if the initial group members are already familiar with one another.

2. Grow slowly so that the group doesn't suddenly feel overwhelmed by new people.

3. Everyone should understand why they are part of the group, and what they bring to it.

Once you've established a group, set ground rules and be sure to enforce them. Remember to keep the security of participants and the moderation of content at the forefront of the activities of the online group.

Figure 1 & II: Moira Whelan, Online Network Development Cheat Sheet, 2020

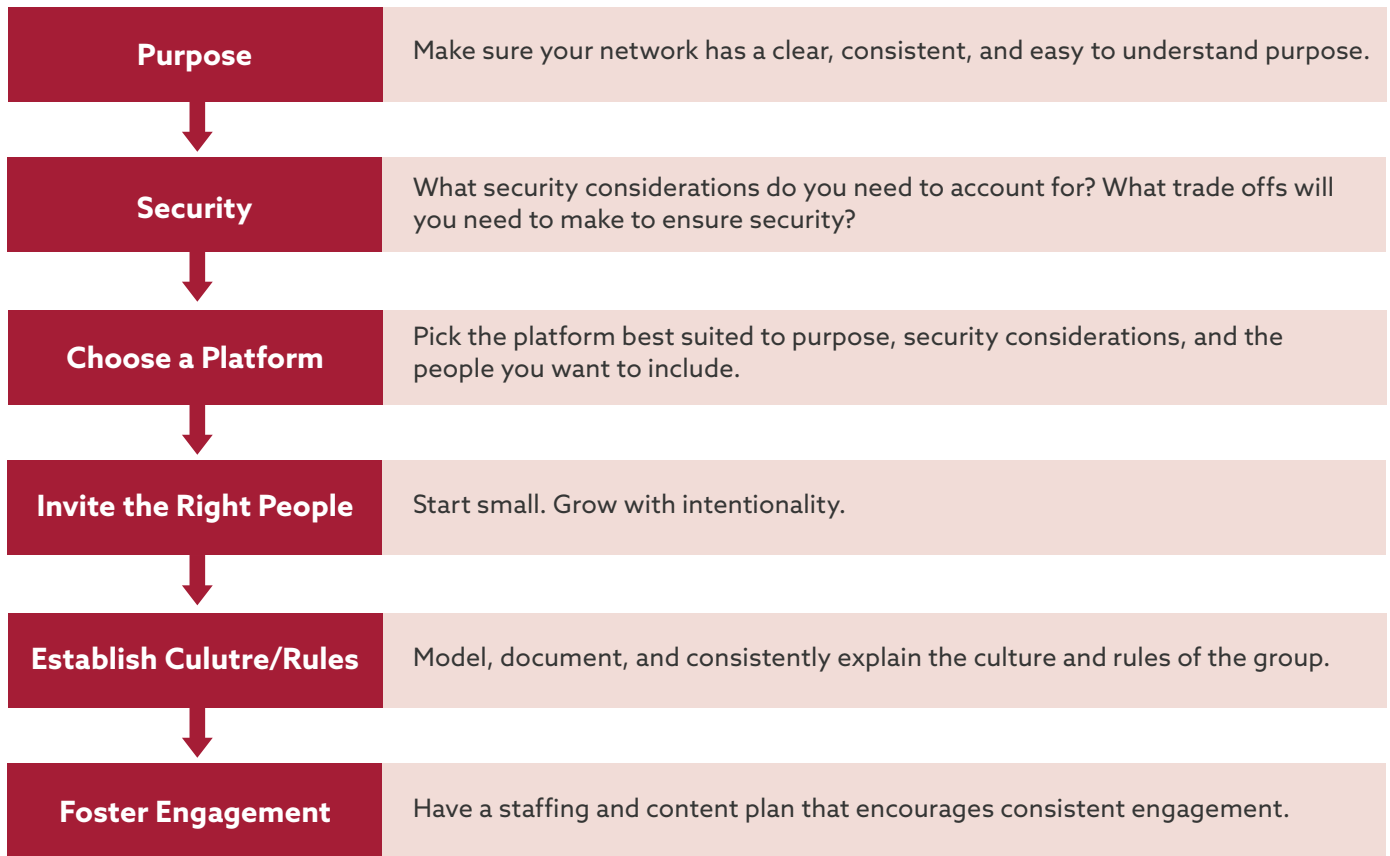|	
Purpose	Make sure your network has a clear, consistent, and easy to understand purpose.
Security	What security considerations do you need to account for? What trade offs will you need to make to ensure security?
Choose a Platform	Pick the platform best suited to purpose, security considerations, and the people you want to include.
Invite the Right People	Start small. Grow with intentionality.
Establish Culutre/Rules	Model, document, and consistently explain the culture and rules of the group.
Foster Engagement	Have a staffing and content plan that encourages consistent engagement.

Figure III: Moira Whelan, Online Network Development Cheat Sheet, 2020

APPENDIX

Appendix I: Safely Conducting Legislative Business in Person during a Public Health Crisis

In situations where legislative business cannot be conducted remotely and in-person meetings are necessary, it is important to strictly follow public health guidelines to keep all participants safe and to demonstrate awareness of how disease or illnesses are spread. Follow simple, but critical, steps to reduce risk at each meeting or event, televised or otherwise. The following information was first provided by the World Health Organization in reaction to the COVID-19 pandemic. Please note that the following recommended measures are not guaranteed to prevent the spread of illnesses, and should be supplemented with additional research and guidance from myriad other trusted, reliable and regularly updated sources.

How COVID-19 spreads: When someone who has COVID-19 coughs or exhales, they release droplets of infected fluid. Most of these droplets fall on nearby surfaces and objects, such as desks, tables or telephones. People could catch COVID-19 by touching contaminated surfaces or objects and then touching their eyes, nose or mouth. If they are standing within one meter of a person with COVID-19, they can catch it by breathing in droplets coughed out or exhaled by them. In other words, COVID-19 spreads in a similar way to the flu. Most persons infected with COVID-19 experience mild symptoms and recover. However, some go on to experience more serious illness and may require hospital care. Risk of serious illness rises with age; people over 40 seem to be more vulnerable than those under 40. People with weakened immune systems and people with conditions such as diabetes, heart disease and lung disease are also more vulnerable to serious illness. This means that it is critical to keep surfaces (e.g., desks and tables) and objects (e.g., telephones and keyboards) clean by regularly wiping them with disinfectant.

Key considerations to prevent or reduce public health risks *before* the meeting or event:

- Develop and agree to a preparedness plan to prevent infection at your meeting or event.
    - Consider whether the meeting or event could be scaled down so that fewer people attend.
    - Ensure and verify information and communication channels in advance with key partners such as public health and healthcare authorities.
    - Pre-order sufficient supplies and materials, including tissues and hand sanitizer for all participants. Have surgical masks available to offer anyone who may need them.

- Actively monitor where COVID-19 is circulating. Advise participants in advance that they should not attend if they have any symptoms or feel unwell.

- Make sure all organizers, participants, caterers and visitors at the event provide contact details: mobile telephone number, email and address where they are staying. State clearly that their details will be shared with local public health authorities if any participant becomes ill with a suspected infectious disease. If they will not agree to this, they cannot attend the event or meeting.

■ Develop and agree a response plan in case someone at the meeting becomes ill with symptoms of COVID-19 (dry cough, fever, malaise). This plan should include at least:

- Identify a room or area where someone who is feeling unwell or has symptoms can be safely isolated.

- Have a plan for how they can be safely transferred from there to a health facility.

- Know what to do if a meeting participant, staff member or service provider tests positive for COVID-19 during or just after the meeting.

- Agree to the plan in advance with your partner healthcare provider or health department.

During the meeting or event:

■ Implement social distancing and increased sanitary and precautionary measures:

- Do not shake hands or engage in physical contact in any way.

- Wear face coverings over both nose and mouth.

- Arrange seats or stand in a manner to ensure participants are at least one meter apart.

- Encourage participants to cover their face with the bend of their elbow or a tissue if they cough or sneeze. Supply tissues and closed bins in which to dispose of them.

- Encourage participants to avoid touching their face altogether.

- Encourage regular hand washing or use of an alcohol rub by all participants at the meeting or event.

■ Display dispensers of alcohol-based hand rub prominently around the venue.

■ Open windows and doors whenever possible to make sure the venue is well ventilated.

After the meeting:

1. Retain the names and contact details of all participants for at least one month. This will help public health authorities trace people who may have been exposed to COVID-19 if one or more participants become ill shortly after the event.

2. If someone at the meeting or event was isolated as a suspected COVID-19 case, the organizer should let all participants know this. They should be advised to monitor themselves for symptoms for 14 days and take their temperature twice a day.

3. If they develop even a mild cough or low-grade fever (i.e., a temperature of 37.3 degrees Celsius or more) they should stay at home and self-isolate. This means avoiding close contact (1 meter or nearer) with other people, including family members. They should also telephone their healthcare provider or the local public health department, giving them details of their recent travel and symptoms.

Appendix II: Checklist for Organization of Online Parliamentary Oversight Hearings

	Action	Timeline	Responsible party	Tips
1.	Choose a parliamentary oversight topic and create a working group	During committee session	Committee	Parliamentary oversight topic is selected in compliance with relevant articles of the legislature. Creating a working group is typically a non-obligatory, but preferred practice that creates a separate "brain center" in the committee that will prepare the topic for discussion, inviting outside experts upon necessity.
2.	Conduct an initial study of the topic	From two weeks to one month, depending on volume	Working group	The working group conducts the initial study, reaching the necessity for parliamentary hearings if it is determined necessary to receive information from persons of interest, beneficiaries, civil society organizations and other actors in addition to officials. The need to organize hearings can also arise in cases where the committee desires to inform the public about the oversight topic.
3.	Confirm hearings' topics, dates, times and online platform types, based on preliminary research	During committee session	Committee, based on the proposal of the working group	The day of the hearings should not coincide with legislative session days. The hearings can be streamed online on the official website of the legislature (YouTube link or other option).

4.	Send the decision on the hearings' invitations to the speaker of the legislature	After the decision is made	Committee chair	
5.	Distribute the announcement for online registration of co-reporters on the committee website and in social networks (if the working group decided on open registration of co-reporters)	20 days prior to hearings	Committee	Google Docs can be used for online registration. The registration form should include fields for name, organization, email, phone number, topic of the report, main points of the report and reasoning for choice of reporting candidate.
6.	Online registration of hearings' co-reporters	15–20 days prior to hearings		In this period, those who wish can register as reporters.
7.	Select reporters, co-reporters and other invitees	13–15 days prior to hearings	Working group, based on the working-group experts' presentation	Based on the goal, location and format of the hearings, it may be decided to have open participation, giving everyone who registered a chance to participate, based on the order of registration. It is also possible to specifically define the list of invitees and allow open participation for the rest, taking into account the obligatory participation of the committee MPs and media presence. The number of hearing participants should not exceed the possibilities of the online platform.
8.	Upon necessity, conduct preliminary discussions with possible reporters, beneficiaries and interested individuals	10–13 days prior to hearings	Working group	
9.	Plan hearing procedures	10 days prior to hearings	Expert, based on results of the working-group discussion	
10.	Confirm the list of reporters and invitees, and confirm hearing procedures	During the committee session	Committee, based on a presentation by the working group	

11.	Book hearings on the online platform, and resolve online streaming and interpretation issues (upon necessity)	10 days prior to hearings	Assistant	
12.	Compose invitations for reporters and other invitees	9–10 days prior to hearings	Assistant	Invitation is sent in the committee chair's name. The invitation states the reason for the invitation and the deadline for providing the main points for the report. Receiving as much written documentation as possible before the hearings allows the committee to a) foresee the hearings' process and control it to reach expected results and b) have sufficient basis to give evidence-based conclusions.
13.	Send invitations to reporters, co-reporters and other invitees by email, providing them with login details of the online platform (link, code, password) and the deadline for registration	Nine days prior to hearings	Assistant	
14.	Prepare the announcement about the hearings and the online registration form, then post it on the committee website, distribute via other means and circulate it in the legislature	10 days prior to hearings	Assistant	Google Docs can be used for online registration. Fields for name, organization, email and phone number should be included.
15.	Prepare questions for the reporters	5–9 days prior to hearings	Expert, based on discussion with the working group	Questions should be provided to the chair and members of the committee to ask later.
16.	Prepare a short report for the reporting MP	5–9 days prior to hearings	Reporting MP member of the working group	One of the committee members can give a short report to present the results of the preliminary study and the questions up for discussion. This function can also be performed by the committee chair.

17.	Prepare a package for the press release and the media, and present the message to the public-relations and communications department	Seven days prior to hearings	Expert	
18.	Re-confirm participation of reporters and invitees, and make arrangements with replacements	5–7 days prior to hearings	Assistant, expert	
19.	Receive the main points of reports and other materials	3–5 days prior to hearings and within three days after hearings, if necessary	Assistant	
20.	Host a trial online meeting	Five days prior to hearings	Assistant, working-group members, committee chair/ hearing manager	The trial online meeting can be held by working-group members, consecutively checking all steps, but actual participants are preferred, such as the committee chair, reporters and interpreters.
21.	Finalize online registration, compose the final list of hearing participants, send out email invitations for individuals who registered online, provide login details (link, code, password) and the registration deadline.	Three days prior to hearings	Assistant	
22.	Prepare procedure, questions and other materials for the hearings, and provide them digitally to committee members	Three days prior to hearings	Expert	
23.	Contact reporters as a reminder	Two days prior to hearings	Assistant	
24.	Circulate a sign-in sheet during hearings to record the names, organizations and contact details of participants	On the day of the hearings	Assistant	

25.	Summarize the hearings' process to compose synopsis	On the day of the hearings	Expert	
26.	Compose the closing report project and present it to the committee	10 days prior to hearings	Expert	The goal of the synopsis is to provide committee members with complete information about the results of the hearing. The hearing synopsis is intended only for the committee's use and is not a basis for future oversight activities. A protocol is composed based on the synopsis, which is later posted on the committee website.
27.	Confirm the synopsis and the protocol based on it, and post it on the official website	During committee session	Committee	
28.	Post the main presentations, proposals, conclusions, information and other materials concluding the hearings on the committee website	After the committee session	Committee chair, in agreement with the legislature's president	

DO YOU SEE A WAY TO MAKE THIS PLAYBOOK BETTER?

Are there new technologies or needs we should address?

We want your feedback.

Please share your ideas, feedback, comments and requests by emailing Amanda Zink at **azink@iri.org** so we can continue to improve this resource.

Please also visit the living version of this document housed on Gitbook using **https://international-republican-institu.gitbook.io/going-virtual-a-guide-for-parliaments-1**, which is more frequently updated to reflect changes in the digital environment.