Vol.2022-EIP-96 No.18
2022/6/10

米国政府による ICTS サプライチェーン保護施策：5G のセキュリティと国際競争

山條　朋子 [1]

概要：米国では, ICTS サプライチェーン保護のための施策, 特に中国企業の製品・サービスの排除を狙った施策が 2017 年以降, 加速度的に講じられてきた. FCC は. 5G 推進施策の一環として, 国家安全保障上のリスクから米国の通信ネットワークを保護するための施策を講じている. さらに米政府は, 代替技術の選択肢の一つとして Open RAN に期待を寄せている.

キーワード：ICTS サプライチェーン, 国家安全保障, 5G, Open RAN

Policies and Rules to secure Communications Networks and ICTS Supply Chain in the United States

TOMOKO YAMAJO [†1]

Abstract: The US government has adopted policies and rules to secure communications networks and ICTS supply chain at an accelerated pace since 2017, aiming at eliminating products and services of Chinese companies. The FCC is taking measures to protect US communications networks from national security risks as part of its comprehensive 5G strategy. The US government is looking to Open RAN as an alternative technology option,

Keywords: ICTS Supply Chain, National Security, 5G, Open RAN

1. はじめに

米国では，ここ数年間に情報通信技術・サービス (Information and Communications Technology and Services，以下「ICTS」) のサプライチェーンを保護することを目的とした大統領令，法律，連邦政府機関の施策等が相次いで発表されている．背景には，トランプ政権下で対中強硬策が取られたこと，5G を含む次世代無線分野の国際競争における覇権争いが過熱してきたことなどが挙げられる．

本稿では，ICTS サプライチェーンの保護，その背景にある 5G 国際競争に関する米政府の方針や施策について，米連邦通信委員会（Federal Communications Commission，以下「FCC」)）の動向を中心に考察する．

2. トランプ政権以降の主な動き

2.1 トランプ政権の方針

米国政府による ICTS サプライチェーン保護のための施策，特に中国企業の製品・サービスの排除を狙った施策は，2017 年以降，加速度的に講じられている．これは，もともと米政府内に根強くあった中国による脅威への懸念が，共和党トランプ政権下でさらにエスカレーションし，より具体化したと捉えられている．特に象徴的な出来事としては以下が挙げられる．

- 2016 年大統領選の選挙期間中に，ドナルド・トランプ候補（当時）が対中強硬策を公約に掲げる
- 2017 年 5 月，米通商代表部代表に対中強硬派のロバート・ライトハイザー氏が就任
- 2017 年 12 月発表の国家安全保障戦略において，中国を「戦略的競争者」と表現[1]
- 2018 年 4 月，米商務省は ZTE への米国製品・技術の供給を禁止[2]
- 2018 年 8 月成立の 2019 年国防権限法（National Defense Authorization Act，以下「NDAA」2019）において，連邦政府と契約する業者が Huawei, ZTE 等の中国企業の製品・サービスを使用することを禁止[3]
- 2019 年 5 月，商務省は Huawei 及びその関連会社への米国製品・技術の供給を禁止[4]

トランプ大統領（当時）は，2019 年 5 月，米国内の ICTS に対する脅威に関して国家非常事態であることを宣言する大統領令を発出し[5]，商務長官に対し，米国及び米国民の安全に受け入れ難いリスクをもたらす外国企業との取引を禁じる権限を付与した．特定の国や企業名は挙げられていないものの，Huawei や ZTE を事実上排除する措置と認識されている．

大統領令を受け，商務省は 2019 年 11 月，ICTS サプライチェーン保護のための規則案を公表して意見募集を行い，

1 (株)KDDI 総合研究所
KDDI Research, Inc.

2021 年 1 月, 暫定最終規則を発表した[6]. 主な内容は以下のとおりである. 本規則は同年 3 月より施行された.

- 商務長官は, 外国の敵対者に所有, 支配またはその管轄・指示の下にある者によって設計, 開発, 製造または供給された ICTS 取引（買収, 輸入, 移転, 導入, 取扱いまたは利用）が, 過度のまたは容認できないリスクをもたらすかどうかをケースバイケースで評価し, 取引の禁止またはリスク軽減措置を指示する.
- 対象敵対者 : 中国（香港を含む）, ロシア, イラン, 北朝鮮, キューバ及びベネズエラの政治家ニコラス・マドゥロ氏
- 対象取引 :（1）米国の司法権が及ぶ個人・法人または資産に関する取引で,（2）外国または外国人が利害関係を持つ資産を含み,（3）2021 年 1 月 19 日以降に開始, 交渉中, 完了した取引で,（4）6 つの技術分野に関する場合.
- 技術分野 :
  （1）重要インフラ（2013 年の大統領政策指令第 21 号により指定）
  （2）通信ネットワーク, アクセスポイント, システム等に不可欠なソフトウェア, ハードウェア等
  （3）米国人の個人情報を扱うデータホスト, コンピューティングサービスに不可欠なソフトウェア, ハードウェア等
  （4）ネット通信可能なセンサー, ウェブカメラ, 監視装置, ルーター, ドローン等
  （5）インターネット通信用ソフトウェア（アプリを含む）
  （6）AI・機械学習, 量子コンピュータ, ドローン, 自律システム, 先端ロボット等に関する ICTS

2.2 バイデン政権の方針

政権発足から間もない 2021 年 2 月, ジョー・バイデン大統領は, ICT を含む重要サプライチェーンの見直しに向けた大統領令を発出し[7], 連邦政府の関係機関に対し, 以下のとおり, 重要製品及び産業分野のレビューを実施するように指示した.

- 4 つの重要製品（半導体, 大容量バッテリー, 重要鉱物, 医薬品）のサプライチェーン : 100 日間のレビュー
- 6 つの重要産業分野（防衛, 公衆衛生, ICT, エネルギー, 輸送, 農産物・食糧生産）のサプライチェーン : より広範囲な 1 年間のレビュー

ICT サプライチェーンに関するレビューは, 商務省と国土安全保障省が共同で担当することとされた. 両省は, 通信ハードウェア, コンピューティングとデータストレージハードウェア, エンドユーザデバイス, オープンソースソフトウェアとファームウェアを含む重要ソフトウェアをサポートするサプライチェーンの評価を実施し, 2022 年 2 月, 評価結果をまとめた報告書を発表した[8]. 報告書では, ICT サプライチェーンを混乱させる恐れのある主要なリスクや課題として, 多くの製品カテゴリの国内生産能力の不足, 単一ソースおよび地域のサプライヤーへの過度の依存, 堅牢なサイバーセキュリティ慣行の限られた使用, 国内労働力への過小投資などを列挙している. その上で, これらのリスクを軽減し, ICT サプライチェーンのレジリエンシーを強化するための策として, 米国内の ICT 製造拠点の活性化, 国際パートナーとの連携強化, ICT 人材パイプラインの強化等の様々な戦略を提言している. また報告書は, 連邦議会に対し, 商務省内にサプライチェーンオフィスを設置することを認め, 予算を割り当てるよう求めている. このオフィスの役割については, 国土安全保障省と協議して, サプライチェーンの脆弱性を特定, 監視および対処し, 業界, 労働者やその他の官民の利害関係者と連携して, ICT 業界全体のレジリエンスを強化することとされている.

2021 年 5 月,バイデン大統領は, トランプ前大統領による ICTS サプライチェーンへの脅威に関する非常事態宣言を延長することを決定した. 同年 6 月には, 上記非常事態に対処するため, 外国の敵対勢力から米国人の機密情報を保護するための大統領令を発出し[9], 中国製アプリの利用禁止などを指示した前政権の大統領令 3 件を撤回する一方, 商務省に以下を命じ, 新たな施策を講じるよう促した.

- 商務長官は, 他の関連省庁と協議の上, 米国人の機密データ（個人を特定できる情報, 健康情報, 遺伝情報を含む）の無制限の販売, 移転またはアクセスによる被害, 外国の敵対者によって所有または管理されている, あるいはその管轄または指示の下にある者による大規模なデータリポジトリへのアクセスによる被害から保護する方法についての勧告をまとめたレポートを 120 日以内に提出する.
- 商務長官は他の関連省庁と協議の上, 外国の敵対者によって, または外国の敵対者の管轄または指示の下で, 所有または管理されている者によって設計, 開発, 製造または供給されるコネクテッドソフトウェアアプリに関連するリスクに対処するため, 追加的な行政及び立法措置を勧告するレポートを 180 日以内に提出する.

3. 通信ネットワークからの中国ベンダー排除

3.1 ユニバーサルサービス基金と絡めた FCC の施策

FCC は, 2018 年 9 月に発表した包括的な 5G 戦略, 「5G FAST Plan」をベースに, 周波数確保, インフラ展開支援, 旧式の規制の撤廃・緩和等の施策を推進している. それらに加え, 国家安全保障上のリスクから米国の通信ネットワークを保護するという課題に取り組んでいる[10].

2018 年 4 月, FCC は, 自らが管轄する連邦ユニバーサルサービス基金と絡めた新たな対策を打ち出した. FCC は, ある設備ベンダーによる米国の通信インフラに対する脅威は, 行政府及び連邦議会にとって長年にわたり懸念事項となっていると指摘し, 米国の通信ネットワークやサプライチェーンに対して国家安全保障上の脅威を与える企業からの製品調達に, ユニバーサルサービス基金の補助を充てることを禁止する規則を提案し, 関係者の意見募集に着手した[11].

2019 年 11 月, FCC は上記提案に基づき, ユニバーサルサービス基金の補助を用いて, 国家安全保障への脅威とみなされる企業から製品やサービスを調達することを禁止する規則を決定した[12]. FCC は, 当初の対象企業として Huawei 及び ZTE を指定することを提案するとともに, 将来的に対象企業を追加するための手続きも制定した. また FCC は, ユニバーサルサービス基金の補助を受ける通信事業者が現在 Huawei 及び ZTE 製品を利用している場合, これらの製品の撤去・置換を義務付けることを提案し, 撤去・置換に伴う費用負担の方法などについて改めて関係者の意見募集を行うこととした.

2020 年 6 月, FCC は, 米国の通信ネットワーク及びサプライチェーンに国家安全保障上の脅威を与える企業として, Huawei 及び ZTE を指定することを正式に決定した[13]. この決定は即日発効となり, これ以降, ユニバーサルサービス基金の補助を利用して両社の製品やサービスを購入することは禁じられた.

3.2 セキュアネットワーク法の成立

2020 年 3 月, 米国の通信ネットワークから信頼できない通信機器を排除する法案, 「Secure and Trusted Communications Networks Act」（セキュアネットワーク法）が連邦議会で可決され, トランプ大統領（当時）の署名により成立した[14]. 本法では, FCC に対し, 信頼できないサプライヤーからの通信機器やサービスの購入・保守管理に連邦補助金を支給することを禁止するとともに, 小規模通信事業者がセキュアでない既存の機器やサービスを撤去・置換するための費用を補填するプログラムを創設するよう指示している. また同法では, FCC に対し, 2021 年 3 月 12 日までに, 米国及び米国民のセキュリティに受け入れ難いリスクをもたらす通信機器・サービスのリストを公表し, その後もリストを維持することを義務付けた.

3.3 中国製機器の撤去・置換プログラム

2020 年 7 月, FCC はセキュアネットワーク法の義務の一部は既に遂行したことを確認する宣言裁定を採択した. さらに同法に定められた様々な義務を履行するため, 追加規則制定提案告示を発出し, 関係者の意見募集に着手した[15]. 2020 年 12 月, FCC は意見募集を経て, 米国の通信ネットワークの安全性を保護するためのルールを決定した[16]. FCC は, ユニバーサルサービス基金の補助を受ける通信事業者に対し, 連邦議会が予算を割り当てることを条件に, 対象となる通信機器及びサービスをネットワークから撤去し, 適切に処分することを義務付ける一方, 小規模通信事業者が対象の通信機器・サービスを撤去・置換するための費用を補填するプログラム（Secure and Trusted Communications Networks Reimbursement Program, 以下「SCRP」）を創設することとした.

2020 年 12 月末, 新型コロナウイルス救済対策を含む包括予算法（H.R. 133）が成立した[17]. 同法では, SCRP の予算として 18.95 億ドルを FCC に割り当てるとともに, 費用補填の対象事業者の要件について当初の加入者数 200 万以下から 1000 万以下に拡大した.

FCC は包括予算法と整合性を取るため, ルールの一部見直しを進め, 2021 年 7 月, 以下を主な内容とする最終ルールを決定した[18].

- FCC は, 国家安全保障上のリスクに指定された通信機器及びサービスのリストを公表する.
- FCC は, 小規模通信事業者が対象の通信機器・サービスを撤去・置換するための費用を補填するプログラムを創設.
- 費用補填を受けられるのは加入者数 1000 万以下の事業者.
- 費用補填の対象となるのは, Huawei 及び ZTE が製造・提供した全ての通信機器・サービスで, 2020 年 6 月 30 日以前に取得したもの（ユニバーサルサービス基金の補助で購入したものに限定しない）.
- 米国の通信ネットワーク上にセキュアでない機器が存在するかどうかについて, FCC が継続して把握できるよう, 厳密な報告義務を定める.

FCC は, 2021 年 10 月から 2022 年 1 月まで SCRP への申請を受け付け, 期限までに 181 件, 総額約 56 億ドルの申請を受領した[19]. FCC による審査は 2022 年 6 月 15 日まで行われる予定となっている.

3.4 国務省による「クリーンネットワーク」の推進

国務省のポンペオ長官（当時）は, 2020 年 4 月, 重要なデータが Huawei や ZTE 等の信頼できないベンダーの設備を経由しないよう, 国内外の米国外交施設に出入りする全ての 5G ネットワークトラフィックに対して, 「クリーンパス」を要求すると発表した[20]. この目標を推進するため, 国務省は 2020 年 6 月, 情報要請書を発出し, 「5G クリーンパス」を実現するシステム, ソリューション, サービスをいかに導入するかについて関係者の意見募集を実施した.

さらにポンペオ長官は, 2020 年 8 月, 5G クリーンパスを拡大した「クリーンネットワーク」プログラムを発表し[21], 中国共産党など悪意のある攻撃者から米国民のプライバシ

ーと企業の機密情報を保護するため，新たな 5 つの取り組みを以下のとおり提示した．

- クリーンキャリア : 信頼できない中国キャリアが米国の通信ネットワークに接続することを禁止．このような企業は米国の国家安全保障に危険をもたらすため，米国との間で国際電気通信サービスを提供すべきではない．
- クリーンストア : 米国のモバイルアプリストアから信頼できないアプリケーションを削除．中国製アプリは，プライバシーを脅かし，ウイルスを増殖させ，プロパガンダや偽情報を拡大．
- クリーンアプリ : 信頼できない中国スマートフォンメーカーが，自社のアプリストアで信頼できるアプリをプレインストールまたはダウンロード可能とすることを禁止．米国及び外国の主要企業は，Huawei のアプリストアからアプリを削除すべき．
- クリーンクラウド : 米国民の機密性の高い個人情報及び COVID-19 ワクチン研究を含む米企業の貴重な知的財産が，Alibaba, Baidu , Tencent 等の企業を通じて海外の敵対者がアクセス可能なクラウドベースのシステムに保存され，処理されることを防止．
- クリーンケーブル : 海外のパートナーとも協力し，米国及び世界の海底ケーブルが中国による大規模な情報収集によって危険にさらされないようにする．

国務省は，クリーンネットワークプログラムの法的根拠を明確にしていない．また同省は，自社のネットワーク内で信頼できないベンダーを使用していないという通信事業者の声明に基づき，「クリーンテレコム（Clean Telco）」のリストを作成し，公表したが，これについてもリストに掲載されるための要件や検証プロセス等は示されていない．従って，国務省によるこれらの取り組みは，法律に基づく他の規則に比べるとやや非公式の扱いであり，その義務は限定的なものと捉えられている．

バイデン政権において，クリーンネットワークプログラムの位置付けは明確にされていない．国務省では，2022 年 4 月，アントニー･ブリンケン国務長官が掲げる米国外交の近代化の一環として，サイバースペース・デジタル政策（CDP）局が新たに発足した[22]．同局の所掌は，サイバースペースやデジタル技術・政策に関連した国家安全保障上の課題，経済的機会，民主主義的価値の推進等とされており，今後，5G ネットワークのセキュリティやサイバースペースでの適切な行動に関する国際規範の確立といった課題に対処していくと見られている．

4. 「Open RAN」の推進

「Open RAN（Radio Access Network）」とは，オープンな使用に基づき，様々なベンダーの機器を自由に組み合わせて利用可能とする，標準化された無線アクセスネットワークである．米政府は，国家安全保障上の懸念をもたらす中国製機器の排除を進める一方，代替技術の選択肢の一つとして Open RAN の導入を推進している．

4.1 FCC の取り組み

2020 年 9 月，FCC は Open RAN をテーマにした最初のイベントとして「Forum on 5G Open Radio Access Networks」を開催した[23]．開会の挨拶に登壇したポンペオ国務長官（当時）は，中国共産党はその技術力を用いて世界中で自由や民主主義を脅かそうとしていると指摘した上で，国務省が推進するクリーンネットワークプログラムに言及し，同盟国に対し，中国共産党と関係のあるベンダーではなく，信頼できる 5G ベンダーを選択するよう訴えた．続いて FCC は，2021 年 7 月に「Open RAN Solutions Showcase」を開催した[24]．その中で FCC のジェシカ・ローゼンウォーセル暫定委員長（当時）は，高度無線通信・ネットワークの研究開発のためのイノベーションゾーンをボストンなどに設置し，米国における Open RAN 市場の開拓を推進する考えを表明した．

2021 年 3 月，FCC は Open RAN の可能性や課題について正式に検討を開始することを決定し[25]，次のような論点を挙げて関係者からの情報収集を実施した．

- 米国及び海外における Open RAN の開発，導入に関する現在の状況
- FCC が Open RAN 技術の成功をどのように醸成し，市場の競争や新規参入をどのように支援すべきか
- Open RAN ネットワークを幅広く，大規模に導入するためにどのようなステップが必要か
- この新技術のネットワークアーキテクチャの標準化における既存の大手メーカーと新規参入者の役割
- Open RAN 標準開発のタイムラインを加速するために FCC，関連する連邦政府機関，産業界，学術界などが取るべき措置
- Open RAN 仕様に基づくシステムの導入，統合，テストに関する課題やその他考慮すべき事項
- Open RAN の開発と導入に関するコストとメリット

これに対し，2021 年 5 月末の期限までに 70 件を超えるコメントが提出された．業界団体の CTIA を含む米モバイル業界は，Open RAN を導入については事業者の自主的な取り組みに任せ，政府は介入すべきではないという意見で概ね一致している．一方，Mavenir Systems, TIP, Rakuten Mobile 等の Open RAN 推進派は，Open RAN 技術の開発や導入を促進するような施策を積極的に講じるよう，FCC に求めている．

2021 年 7 月，バイデン大統領は，米国経済の競争を促進するための大統領令を発出し[26]，競争を増加させるための策として，労働，医療，運輸，農業，金融，インターネッ

ト，技術などの分野において，10 以上の連邦政府機関が早急に取り組むべき 72 のイニシアチブを提示した．その一環として，競争，低廉な料金，活況でイノベーティブな電気通信エコシステムを促進するための策として，FCC に対し，5G Open RAN ネットワークの開発や導入を引き続きサポートし，5G 機器市場におけるオープン性，イノベーション及び競争を促進するような施策を講じることが奨励されている．

4.2 Open RAN 推進のための基金

2021 年 1 月，国防予算の大枠を定める「2021 年国防権限法（NDAA 2021）」が成立した[27]．同法には，連邦議会上院の情報特別委員会委員長を務めるマーク・ワーナー議員（民主党）と同委員会メンバーのマルコ・ルビオ議員（共和党）の働きかけにより，Open RAN 技術の開発や機器の採用を促進するため，「Public Wireless Supply Chain Innovation Fund」（イノベーション基金）及び「Multilateral Telecommunications Security Fund」（セキュリティ基金）を設立することが盛り込まれた．

両議員を含む上院情報特別委員会の超党派議員 15 名は，2021 年 4 月，バイデン大統領に対し，Open RAN 機器の採用を促すため，上記 2 つの基金に 15 億ドルずつの予算を割り当てることを要求する連名の書簡を送付した[28]．書簡の中で議員らは，中国政府と密接な関係を持ち，米国企業の知的財産権を軽視してきた歴史を持つ Huawei は，エンドツーエンドの RAN ハードウェアを提供しており，重大な防諜上の懸念を引き起こしていると警告している．さらに，議員らは，米国はこの数年間，米国の通信事業者や同盟国に対し，Huawei の 5G 技術を排除するよう呼びかけてきたが，価格競争力のある革新的な代替案を示せていないと指摘し，Open RAN のアーキテクチャにより，サプライチェーンを多様化し，海外サプライヤーへの依存度を引き下げることができるとして，予算の必要性をアピールしている．

イノベーション基金については，米国イノベーション・競争法（2021 年 6 月に上院通過）により 15 億ドルの予算を計上されたが，これまでのところ，セキュリティ基金の予算措置は講じられていない．

5. おわりに

ICTS サプライチェーンの保護は超党派の案件であり，民主党バイデン政権においても重要分野の一つと位置付けられている． 前政権時代から大きな方針転換はないものの，同盟国との連携や国際協調を重視するバイデン政権の特徴的なアプローチが，この分野においても採用されている．2021 年 9 月に開催された日米豪印首脳会合，通称「QUAD」では，重要・新興技術を発展させる新たな取り組みの一環として，5G 展開・多様化を支持し，Open RAN の展開及び採用を促進していくことが合意された．

FCC は，米国の通信ネットワークから Huawei 及び ZTE 製品・サービスを撤去・置換するため，これらの製品・サービスの主な利用者である中小規模事業者への費用補填プログラムを立ち上げた．予算を大幅に上回る申請があったことから，連邦議会による追加の予算措置が避けられない事態となっている．予算の確保に加えて，Huawei・ZTE 製品を撤去・置換する事業者に，Open RAN を含め，信頼できる代替技術の新たな選択肢を用意するという課題が，米政府にとって今後ますます重要度を増すと考えられる．

参考文献

[1] The White House, National Security Strategy of the United States of America (December 2017) https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[2] Department of Commerce, ZTE Denial Order https://www.commerce.gov/files/zte-denial-order
[3] H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 https://www.congress.gov/bill/115th-congress/house-bill/5515/text
[4] Department of Commerce, Bureau of Industry and Security, Addition of Entities to the Entity List (May 21, 2019) https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list
[5] The White House, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019) https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/
[6] Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (01/19/2021) https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain
[7] The White House, Executive Order on America's Supply Chains (February 24, 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
[8] Department of Commerce, ICT Supply Chain Assessment Fact Sheet (February 24, 2022) https://www.commerce.gov/news/fact-sheets/2022/02/ict-supply-chain-assessment-fact-sheet
[9] The White House, Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries (June 9, 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/
[10] FCC, America's 5G Future https://www.fcc.gov/5G
[11] FCC Proposes to Protect National Security Through FCC Programs (Apr 18, 2018) https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0
[12] FCC, Protecting National Security Through FCC Programs (Nov

26, 2019)
https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0
[13] FCC Designates Huawei and ZTE as National Security Threats (June 30, 2020)
https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats
[14] H.R.4998 - Secure and Trusted Communications Networks Act of 2019
https://www.congress.gov/116/plaws/publ124/PLAW-116publ124.pdf
[15] FCC, Implementing the Secure Networks Act (July 17, 2020)
https://www.fcc.gov/document/implementing-secure-networks-act-0
[16] FCC Adopts Rules to Secure Communications Networks and Supply Chain (December 11, 2020)
https://www.fcc.gov/document/fcc-adopts-rules-secure-communications-networks-and-supply-chain-0
[17] H.R. 133 - Consolidated Appropriations Act, 2021
https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-116HR133SA-RCP-116-68.pdf
[18] FCC Acts to Protect National Security in Communications Supply Chain (July 14, 2021)
https://www.fcc.gov/document/fcc-acts-protect-national-security-communications-supply-chain-0
[19] FCC Announces Supply Chain Reimbursement Program Applications Filed (February 9, 2022)
https://www.fcc.gov/document/fcc-announces-supply-chain-reimbursement-program-applications-filed
[20] Department of State, Secretary Michael R. Pompeo At a Press Availability (April 29, 2020)
https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/index.html
[21] Department of State, Secretary Michael R. Pompeo At a Press Availability (August 5, 2020)
https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-10/index.html
[22] Department of State, Establishment of the Bureau of Cyberspace and Digital Policy (April 4, 2022)
https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/
[23] FCC, Forum on 5G Open Radio Access Networks (September 14, 2020)
https://www.fcc.gov/news-events/events/forum-5g-virtual-radio-access-networks
[24] FCC, Open RAN Solutions Showcase (July 14-15, 2021)
https://www.fcc.gov/news-events/events/2021/07/open-ran-solutions-showcase-day-1
https://www.fcc.gov/news-events/events/2021/07/open-ran-solutions-showcase-day-2
[25] FCC Seeks Comment on Open Radio Access Networks (May 18, 2021)
https://www.fcc.gov/document/fcc-seeks-comment-open-radio-access-networks-0
[26] The White House, Executive Order on Promoting Competition in the American Economy (July 9, 2021)
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/
[27] H.R.6395 - William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021
https://www.congress.gov/bill/116th-congress/house-bill/6395
[28] Sen. Mark R. Warner, Bipartisan Senators Urge Funding for Secure 5G Networks (April 6, 2021)
https://www.warner.senate.gov/public/index.cfm/pressreleases?id=C2472F4B-0A08-4454-80F9-2299AA0BE419